THE THREAT REPORT

Fall 2022

Presented by

Trellix ADVANCED RESEARCH CENTER

چکیده مدیریتی

به گزارش فصلی شرکت ترلیکس (Trellix) خوش آمدید!

این اولین گزارش فصلی ترلیکس است که توسط مرکز تحقیقات پیشرفته این شرکت (Trellix Advanced Research Center) ارائه می‌شود.

راه‌اندازی مرکز تحقیقات پیشرفته ترلیکس در تابستان امسال نقطه عطف مهمی در مسیر حرکت شرکت نوظهور ترلیکس است. این مرکز، متشکل از صدها تحلیلگر و محقق امنیتی نخبه، عهده‌دار مسئولیت کمک به مشتریان در شناسایی جدیدترین تهدیدات امنیت سایبری و پاسخگویی مؤثر به آنها است.

در این گزارش به بررسی تهدیدات سایبری در سه‌ماهه سوم ۲۰۲۲ پرداخته شده است.

تهدیدات سایبری در بازه زمانی مذکور همچنان خبرساز بودند. همان طور که در این گزارش خواهید خواند در سه‌ماهه سوم شاهد تشدید رویدادهای سایبری، افزایش پیچیدگی فنی حملات و تأثیرات آنها بر روی حوزه‌های اقتصادی و ژئوپلیتیکی بودیم.

در سه‌ماهه سوم، باج‌افزار LockBit بیشترین انتشار را در مقایسه با هم‌قطاران خود داشته است. Cobalt Strike و Mimikatz نیز پراستفاده‌ترین ابزارهای مخرب در این دوره بوده‌اند.

بررسی‌های مرکز تحقیقات پیشرفته ترلیکس نشان می‌دهد که Mustang Panda، فعال‌ترین گروه APT در سه‌ماهه سوم ۲۰۲۲ بوده است. APT29 و APT36 از دیگر گروه‌های فعال در دوره مذکور بودند که در گزارش ترلیکس به ترتیب در جایگاه دوم و سوم قرار گرفته‌اند.

همچون دوره‌های قبلی در این گزارش نیز آماری از روش مخرب "کسب روزی از زمین" (Living off the Land - به اختصار LotL) پرداخته شده است. در روش LotL مهاجمان از برنامه‌های عادی و سالم در سیستم قربانی برای انجام عملیات مخرب خود بر روی آن دستگاه استفاده می‌کنند. بدیهی است که این روش برای مخفی ماندن عملیات مخرب و شناسایی نشدن حملات بسیار مؤثر است. بر طبق گزارش ترلیکس، دو پروسه معتبر CMD و PowerShell بیشترین سهم بهره‌جویی توسط مهاجمان را به خود اختصاص داده‌اند.

در بخشی دیگر از این گزارش نیز اصلی‌ترین تهدیدات مبتنی بر ایمیل در سه‌ماهه سوم ۲۰۲۲ مورد بررسی قرار گرفته است.

ادغام شرکت مک‌آفی اینترپرایز (McAfee Enterprise) و شرکت فایرآی (FireEye) به‌عنوان دو قدرت امنیت فناوری اطلاعات تحت برند ترلیکس که در اواخر سال گذشته رخ داد نویدبخش آینده‌ای روشن در مقابله با تهدیدات سایبری است. ضمن آن که اطلاعات انبوه شرکت جدید ترلیکس و دامنه گسترده محصولات و مشتریان آن در سرتاسر جهان چشم‌اندازی دقیق را از وضعیت تهدیدات سایبری فراهم می‌کند.

گروه تحقیق و توسعه

شرکت مهندسی شبکه گستر - اولین شرکت فعال در حوزه ضدویروس در ایران

www.shabakeh.net

ABOUT THE TRELLIX ADVANCED RESEARCH CENTER

The Trellix Advanced Research Center has the cybersecurity industry's most comprehensive charter and is at the forefront of emerging methods, trends, and actors across the threat landscape. The premier partner of security operations teams across the globe, The Trellix Advanced Research Center provides intelligence and cutting-edge content to security analysts while powering our leading XDR platform.

ABOUT TRELLIX

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confident in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerated technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at www.trellix.com.

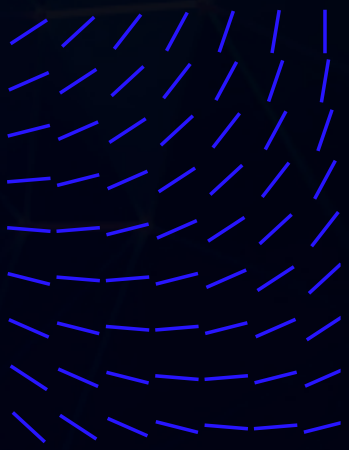


TABLE OF CONTENTS

Q3 2022 THREAT OVERVIEW

In the third quarter of 2022, Trellix delivered a new, powerful resource to support the future of extended detection and response (XDR) and cybersecurity. The Trellix Advanced Research Center, comprised of hundreds of elite security analysts and researchers was established to help customers detect, respond, and remediate the latest cybersecurity threats.

Threat actors also made headlines in Q3 2022 and our Advanced Research Center team countered with research and findings on a global scale. Our team took you through the dismantling of REvil including the steps taken to build their cybercriminal enterprise and the missteps that led to their downfall. The Advanced Research Center revealed what the code told us, the All-Star lineup and followed the money to REvil's end. When United States Speaker of the House Nancy Pelosi visited Taiwan, our team examined the news-making geopolitical tensions after detecting a spike in regional cyber threat activity targeting the Taiwan government.

This first Threat Report presented by the Trellix Advanced Research Center, showcases the rapid research and real-time intelligence resources with notable data and findings from Q3 2022 including:

- Increased threats to Transportation and Shipping sectors.
- Increased threats to Germany.
- The proliferation of old CVEs – from 2016, 2017, 2018 – as the most commonly exploited in 2022.

LETTER FROM OUR HEAD OF THREAT INTELLIGENCE

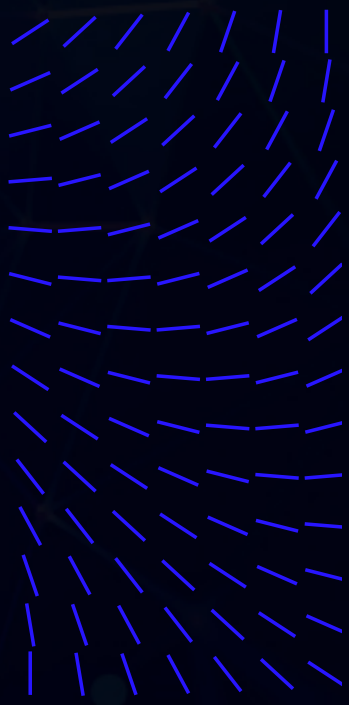
Welcome to the first Threat Report from the Trellix Advanced Research Center.

The launch of our Advanced Research Center this September was an important milestone in our trajectory since emerging as Trellix earlier this year. Our goal is to identify and illuminate a broad spectrum of threats in today's complex landscape through research in nearly every vertical of threat, including those targeting governments, financial, retail, manufacturing, critical infrastructure, healthcare, industrial controls, and many other industries. The Advanced Research Center consists of a cohesive group of researchers with purpose: to produce actionable real-time threat intelligence and world class efficacy to help customers stay protected against the latest cybersecurity threats, while powering our leading XDR platform.

The last quarter saw cyber events continue to intensify in their technical sophistication and in their potential for economic and geopolitical impact. We observed uninterrupted activity out of Russia, Chinese actors targeting Taiwan, North Korean actors launching cyberattacks timed with missile drills, activities not only attributed to state-sponsored groups, but we observed a rise in politically motivated hacktivist activity. All this, plus continued attacks on healthcare and education systems targeted by ransomware gangs along with the shortage of cybersecurity talent around the world now reaching 3.4 million, shows the need for threat intelligence work isn't slowing down.

Since the introduction of our Advanced Research Center, we have published research into a 15-year-old vulnerability impacting 350,000 open-source projects, threats to Taiwan, our efforts to support law enforcement action against members of REvil, the evolution of social engineering tactics used in BazarCall campaigns and phishing attacks targeted U.S. election workers.

With this report, we continue to build our momentum as Trellix's Advanced Research Center stands at the forefront of our industry helping organizations better understand, detect, and respond cyber threats. In addition to the data you have known us to deliver in these



reports, you will see new data from our email research experts and new insights on our Cobalt Strike infrastructure tracker, one of the many cyber-threat trackers we maintain 24/7. As this report sees new iterations each quarter, we will continue to add new insights, metrics, and intelligence. We're just getting started.

If there are topics you would like to see, don't hesitate to reach out to me @John_Fokker or our team @TrellixARC on Twitter. We're ready.

John Fokker
Head of Threat Intelligence

METHODOLOGY

Trellix's backend systems provide telemetry that we use as input for these reports. We combine our telemetry with open-source intelligence around threats and our own investigations into prevalent threats like ransomware, nation-state activity, etc.

When we talk about telemetry, we talk about detections, not infections. A detection is recorded when a file, URL, IP address, or other indicator is detected by one of our products and reported back to us.

Privacy of our customers is key. It is also important when it comes down to telemetry and mapping that out to the sectors and countries of our customers. Client-base per country differs and numbers could be showcasing increases while we have to look deeper into the data to explain. An example: The Telecom sector often scores high in our data. It doesn't necessarily mean this sector is highly targeted. The Telecom sector contains ISP providers as well that own IP-address spaces that can be bought by companies. What does this mean? Submissions from the IP-address space of the ISP are showing up as Telecom detections but could be from ISP clients that are operating in a different sector

As the cybersecurity landscape changes and organizations become more sophisticated, it's important to note that organizations use legitimate indicators in test scenarios to prepare their security operations teams for response. This means that while some data may score high, it may include threat indicators from security preparation exercises.

GLOBAL RANSOMWARE

Q3 2022 Global Ransomware Highlights

- Conti officially stopped their operations. Conti's source code was leaked as well as their chats.
- LockBit remains the top ransomware family. At the end of Q3 their "builder" was released, and allegedly various groups are already establishing their own RaaS with it. Phobos ransomware continues to be active and accounts for 10% of our telemetry hits. Their tactic of selling a complete ransomware kit and avoiding large organizations allows them to stay under the radar.

The following Global Ransomware stats are based on our telemetry (customers logs) correlated with the malicious campaigns collected and analyzed by the Threat Intelligence Group:

MOST REPORTED RANSOMWARE CUSTOMER SECTORS Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several ransomware campaigns. The following industry sectors represent the most impacted by the identified campaigns:

Top Countries, Families, Tools & Techniques

Our global telemetry showed indicators of compromise (IoCs) that belong to several ransomware campaigns. The following countries represent the most impacted by the identified campaigns:

+32%

Germany showed an increase of 32% of identified ransomware campaigns from Q2 to Q3 2022, while the United States realized a 9% increase and Israel showed a 52% decrease in identified campaigns for the same period.

GLOBAL RANSOMWARE FAMILY DETECTIONS Q3 2022

1.	LockBit	22%
2.	HelloXD (Babuk Source code leak Spin off)	11%
3.	Zeppelin	11%
4.	Phobos	10%
5.	BlackCat	10%

MALICIOUS TOOLS USED IN GLOBAL RANSOMWARE CAMPAIGNS Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several ransomware campaigns. The following malicious tools represent the most used in the identified campaigns:

1.	Cobalt Strike	33%
2.	Mimikatz	22%
3.	RCLONE	10%
4.	BloodHound	7%
5.	WinPEAS	6%

MOST REPORTED RANSOMWARE MITRE ATT&CK TECHNIQUES Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several Ransomware campaigns. The following MITRE ATT&CK Techniques represent the most utilized in the identified campaigns:

1. Data Encrypted for Impact
2. System Information Discovery
3. File and Directory Discovery
4. Inhibit System Recovery
5. Service Stop

27%

Germany ranked highest among countries impacted by indicators of compromise (IoCs) in Q3 2022, comprising 27% of top-10 impacted countries by the identified ransomware campaigns.

U.S. Ransomware Sectors Q3 2022

The following stats are based on our telemetry correlated with the malicious campaigns that the Trellix Advanced Research Center collected and analyzed in Q3 2022. Our telemetry on U.S. customers showed indicators of compromise (IoCs) that belong to several ransomware campaigns. The following industry sectors represent the most impacted by the identified campaigns:

38%

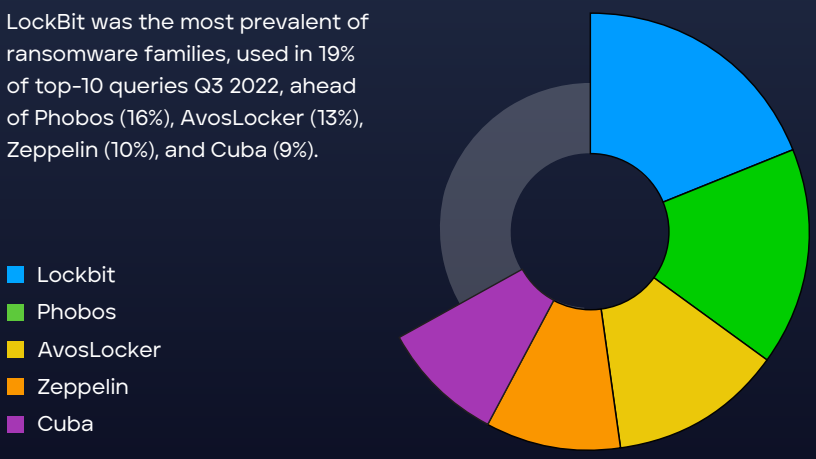
Business Services accounted for 38% of total ransomware detections among the top-10 sectors in the United States in Q3 2022, ahead of Transportation and Shipping (23%), Telecom (9%), Government (9%), and Media and Communications (9%).

+100%

Detections in the Transportation & Shipping sector (all modes including trucking and aviation) increased 100% from Q2 to Q3 2022. Notable increases and decreases include Telecom (+56%) and Finance (-59%).

U.S. RANSOMWARE FAMILIES Q3 2022

LockBit was the most prevalent of ransomware families, used in 19% of top-10 queries Q3 2022, ahead of Phobos (16%), AvosLocker (13%), Zeppelin (10%), and Cuba (9%).



MOST DETECTED U.S. RANSOMWARE TOOLS Q3 2022

Our telemetry on U.S. customers showed indicators of compromise (IoCs) that belong to several ransomware campaigns. The following malicious tools represent the most used in the identified campaigns:

1.	Cobalt Strike	34%
2.	Mimikatz	22%
3.	RCLONE	10%
4.	Bloodhound	6%
5.	Grabff	6%

MOST DETECTED MITRE ATT&CK TECHNIQUES Q3 2022

Our telemetry on U.S. customers showed indicators of compromise (IoCs) that belong to several ransomware campaigns. The following MITRE ATT&CK Techniques represent the most utilized in the identified campaigns:

1. Data Encrypted for Impact
2. System Information Discovery
3. File and Directory Discovery
4. Modify Registry
5. Process Discovery

NATION-STATE STATISTICS Q3 2022

These stats are based on our telemetry correlated with the malicious campaigns that the Threat Intelligence Group within our Advanced Research Center collects and analyzes:

MOST ACTIVE APT GROUPS Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several campaigns from advanced persistent threat groups (APT). These threat actor groups are known to use a variety of tools during their campaigns. These tools range from commodity malicious tools, used by numerous actors, to custom malware used exclusively by a particular APT. The following APT Groups represent the most active in the identified campaigns:

- Mustang Panda
- APT 29
- APT36
- MuddyWater
- Turla

Q3 2022 U.S. Ransomware Malicious Tools Highlights

Based on our IOC tracking, Mustang Panda was the most active APT group in Q3 2022.

Nation-State Client Countries, Sectors & Tools Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several campaigns from advanced persistent threat groups (APT). The following countries, sectors, and tools represent the most impacted by the identified campaigns:

29%

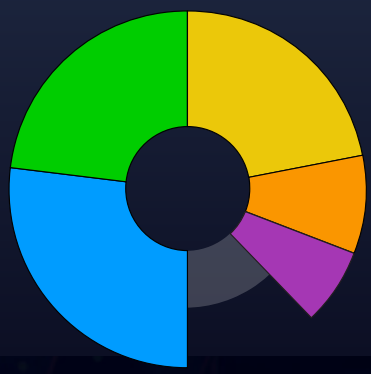
Germany was the most targeted country by APT actors in Q3, comprising 29% of detections among top-to-ranked client countries.

TOP CLIENT COUNTRIES Q3 2022

1.	Germany	29%
2.	United States	16%
3.	Turkey	12%
4.	Israel	10%
5.	India	7%

NATION-STATE SECTORS Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several campaigns from APT groups. The following industry sectors represent the most impacted by the identified campaigns:



- Transportation & Shipping
- Telecom
- Media & Communications
- Technology
- Business Services

NATION-STATE MALICIOUS TOOLS Q3 2022

Our global telemetry showed indicators of compromise (IoCs) that belong to several campaigns from APT groups. The following malicious tools represent the most used in the identified campaigns:

1.	Mimikatz	24%
2.	PlugX	20%
3.	Cobalt Strike	18%
4.	Crimson RAT	7%
5.	Metasploit	6%

EMAIL SECURITY TRENDS Q3 2022

These stats are based on telemetry generated from the several email security appliances installed on customers around the world. The detection logs are aggregated and analyzed to produce the following sections:

TOP VECTORS MOST IMPACTED BY MALICIOUS EMAILS Q3 2022

URL

91%

url comprised 91% of the top-10 most utilized means of packing malicious payloads from all detected malicious emails in Q3 2022.

TOP EMAIL ATTACK CATEGORIES Q3 2022

1.	Phish	68%
2.	Malware	22%
3.	Scam	9%
4.	Exploit	<1%
5.	APT	<1%

TOP EXPLOITED CUSTOMER EMAIL CVES Q3 2022

VULNERABILITIES IMPACTING MICROSOFT OFFICE EQUATION EDITOR

75%

The "equation editor vulnerabilities" comprised by CVE-2017-11882, CVE-2018-0798, and CVE-2018-0802 were the most exploited among malicious emails received by customers in Q3 2022. The exploits that target these vulnerabilities are incorporated in very generic malware families like Formbook, Netwire, and Generic Downloaders.

TOP SECTORS MOST IMPACTED BY MALICIOUS EMAILS Q3 2022

FINANCIAL SERVICES

20%

Financial Services was the sector most impacted by malicious emails in Q3 2022, followed by State and Local Government (13%), Manufacturing (12%), Federal Government (11%), and Services & Consulting (10%)

TROJAN

83%

Trojan comprised 83% of the top-5 most utilized attack categories detected in malicious emails in Q3 2022.

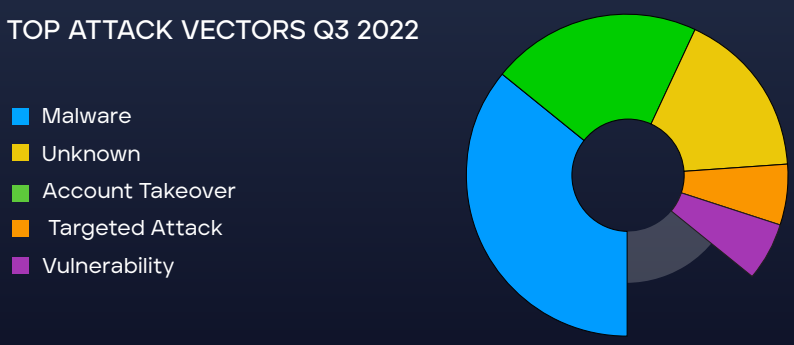
TOP EMAIL MALWARE FAMILIES Q3 2022

1.	Exsto	17%
2.	Agenttesla	16%
3.	Formbook	15%
4.	Leonem	7%
5.	Guloader	7%

COUNTRIES, SECTORS, AND VECTORS Q3 2022

Notable breach data from open-sourced publicly reported incidents in Q3 2022:

TOP ATTACK VECTORS Q3 2022



35%

The United States experienced the most reported incidents (35%) in Q3 2022.

TOP ATTACK SECTORS Q3 2022

1.	Multiple Industries	20%
2.	Individuals	11%
3.	Public	11%
4.	Healthcare	9%
5.	Technology	6%

LIVING OFF THE LAND (LOLBIN) AND THIRD-PARTY TOOLS

OS Binaries Q3 2022

In the third quarter of 2022, threat actors, including APT and ransomware groups, continued to rely on OS binaries to carry out mundane tasks. Living off the Land with the OS binaries such as the Windows Command Shell (CMD) and PowerShell, threat actors can take a more hands-off approach and script phases of a campaign, from initial access, reconnaissance, or exfiltration of targeted information. CMD and PowerShell do continue to be the most prevalent binaries that are abused with scheduled tasks nipping at their heels. Over the last three quarters and throughout 2021 threat actors have made use of the OS binaries in all stages of an attack, from initial access to malware deployment, ingress tool transfers all the way to impact as mapped out on the MITRE ATT&CK Matrix. Loader and downloader may make use of CMD to spawn MSHTA to load a payload or download additional malware or to exfiltrate

system and infrastructure information, scheduled tasks may be used to install webshells to maintain persistent access or kick off the encryption process in a ransomware campaign. APT groups use OS binaries when performing tasks such as the discovery of AD users, groups, and permissions, discovering domain trusts, as well as bypassing security hindrances and elevating privileges. Ransomware campaigns have been seen utilizing OS binaries and third-party tools to steal valid credentials, deploy additional payloads and spawn data collection and exfiltration tasks.

MOST PREVALENT OS BINARIES Q3 2022

1.	Windows Command Shell/CMD	38%
2.	Powershell	37%
3.	Schtasks	21%
4.	WMI/WMIC	18%
5.	Rundll32	13%

Throughout daily operations, we repeatedly see these OS binaries make their way through the attack lifecycle and will continue to report their abuses.

Third-party tools continue to be of interest to threat actors as they pursue the path of least resistance. Remote access tools provide a great resource to threat actors, recently there has been an uptick in red team tools present in campaigns and quite a few tools have been developed to avoid detections that come with tools that have been used for some time such as Cobalt Strike. When threat actors pair the third-party tools, that system administrators and security practitioners may use, with the OS binaries their arsenals grow without much effort. These tools can be used for discovery of network assets, the collection and compression of the data of interest and exfiltration to the threat actor controlled C2 server.

A recent addition to the third-party tools section includes a "Red Team Tools" segment which highlights the red team tools that we see threat actors abusing. These tools may include but are not limited to tools such as Cobalt Strike, BruteRatel, or the Sliver Implant. Over the past few years, the Trellix Advanced Research Center has continuously tracked the presence and abuse of the Cobalt Strike red team tool. Through our tracking we have identified a majority

TOP THIRD-PARTY TOOLS Q3 2022

1.	Remote Access Tools	29%
2.	Red Team Tools	16%
3.	File Transfer	10%
4.	Network Discovery	9%
5.	AD Discovery	4%

Cobalt Strike C2 servers operating throughout Asia, Europe, and North America. Additionally, our threat hunting operations have allowed us to identify license types in use, aggregate the data and attribute the use to licensed, cracked, and stolen versions of Cobalt Strike and attribute their use to clusters of threat actors. Of those identified, just over 56% can be attributed to trial versions of the tool, 26% comes from licensing abused by the EvilCorp and Maze Groups, 17% of operations from licenses abused by UNC1878 (RYUK) with the remaining 1% originating from legitimate security firms, cracked versions, and those abused by the REvil group.

Cobalt Strike was originally developed to be a red team tool that allowed security practitioners to emulate an attack scenario and perform tabletop exercises. Threat actors took notice of the tool's capabilities, and just as hackers will be hackers, repurposed the tool for malicious intent. Cobalt Strike became popular amongst threat groups and soon became the go-to tool as cracked versions found their way into darkweb forums and trail versions into attacks. Development of detection capabilities made it harder to use the tool for both good and nefarious purposes. Other tools such as the Sliver Implant and BruteRatel were developed as alternatives to Cobalt Strike. They are appearing in campaigns, slowly being adopted by threat actors seeking tools with fewer detections to go unnoticed during an attack.

Cobalt Strike continues to be a popular tool of choice amongst threat actors when carrying out tasks from initial access to exfiltration. During the third quarter of 2022 the Trellix Advanced Research Center has seen campaigns ranging from politically motivated threat groups to state-sponsored APTs make use of Cobalt Strike throughout the attack life cycle. The red team tool has also been identified in campaigns where "credential recovery," infrastructure discovery, and exfiltration tasks were carried out prior to the encryption phase by standalone ransomware families as well as ransomware-as-a-service operators. The uptick in use of these third-party red team tools continues as they make their way to the threat landscape, and as such, it is important to make them a part of the tools included in reports when they are present in the top-third-party tools used for attacks.

INSIGHTS RANSOMWARE TRACKING Q3 2022

Ransomware events processed in the Insights platform track the threat actor and tools they abuse. Nearly every ransomware event shows evidence of Living off the Land which includes the abuse OS Binaries present on the system, or the third-party tools used by IT and InfoSec teams to carry out daily tasks. These tools may be abused for automation, task scheduling, privilege escalation, password "recovery" as well as ingress tool transfer. In the third quarter of 2022, where ransomware was the final payload, the number of events processed in the Insights platform stood at just over 15 percent. Some of the campaigns may have contained more than one ransomware family or the ransomware was yet to be identified as of these statistics. The families of ransomware we have listed represent those that have been reported by industry organizations as well as those that are tracked by the Trellix Advanced Research Center. Interestingly, of the several new and surviving ransomware families that continue to make headlines our telemetry shows us that there are still families of ransomware, like Phobos, that continue to be active yet are less visible in public reports.

Ransomware Q3 2022

LockBit Ransomware
BianLian Ransomware
BitLocker
Black Basta Ransomware
BlackByte Ransomware
Maui Ransomware
ROADSWEEP Ransomware
Agenda Ransomware
BlueSky Ransomware
Crytox Ransomware
Cuba Ransomware
FARGO Ransomware
GwisinLocker Ransomware
H0lyGh0st
HavanaCrypt Ransomware
Industrial Spy Ransomware
Karma
LILITH
MedusaLocker
Noberus Ransomware
Ragnar Locker Ransomware
RedAlert
Redeemer Ransomware
Slam Ransomware
SolidBit Ransomware

شبکه گستر
خدمات آگاهی رسانی

Visit Trellix.com to learn more.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

072022-05