VSRC 安全周报（2021-08-31）

0x00 本周漏洞综述

本周需要关注漏洞共 2 个：OpenSSL 缓冲区溢出漏洞（CVE-2021-3711）；F5 8 月多个安全漏洞。

本周安全态势共 3 个：勒索软件 LockFile 利用 ProxyShell 和 PetitPotam 漏洞劫持 Windows 域；2021 年上半年针对 Linux 的常用漏洞 TOP15；Cinobi 银行木马活动分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. OpenSSL 缓冲区溢出漏洞（CVE-2021-3711）

漏洞概况

CVE ID	CVE-2021-3711	时 间	2021-08-24
类 型	缓冲区溢出	等 级	高危
远程利用		影响范围	
攻击复杂度		可用性	
用户交互		所需权限	
PoC/EXP		在野利用	

漏洞详情

2021 年 8 月 24 日，OpenSSL 项目发布安全公告，修复了 OpenSSL 中的一个缓冲区

溢出漏洞（CVE-2021-3711）和一个拒绝服务漏洞（CVE-2021-3712，中危），攻击者可以利用这些漏洞更改应用程序的行为或使应用程序崩溃，导致拒绝服务或敏感信息泄露。

OpenSSL 缓冲区溢出漏洞（CVE-2021-3711）

SM2 解密代码中存在安全问题，第一次调用 EVP_PKEY_decrypt() 返回的明文所需的缓冲区大小的计算可能小于第二次调用所需的实际大小。当应用程序第二次使用较小的缓冲区调用 EVP_PKEY_decrypt() 时，可能会导致缓冲区溢出。恶意攻击者如果能够向应用程序提供用于解密的 SM2 内容，将导致攻击者选择的数据溢出缓冲区最多 62 个字节，改变缓冲区后的其它数据内容，这将改变应用程序的行为或导致应用程序崩溃，但缓冲区的位置取决于应用程序，通常是堆分配的。

影响范围

OpenSSL 1.1.1-1.1.1k

OpenSSL 拒绝服务漏洞（CVE-2021-3712）

如果应用程序要求打印一个 ASN.1 结构，而该 ASN.1 结构包含由应用程序直接构建的 ASN1_STRING，而没有以 NUL 结束 "data "字段，那么就会发生读取缓冲区溢出，同样的问题也可能发生在证书的名称约束处理过程中。如果恶意攻击者可以使一个应用程序直接构建一个 ASN1_STRING，然后通过受影响的 OpenSSL 函数之一进行处理，则能够触发此漏洞，并造成拒绝服务或导致密钥或敏感信息泄露。

影响范围

OpenSSL 1.1.1-1.1.1k

OpenSSL 1.0.2-1.0.2y

安全建议

目前这些漏洞已经修复，建议及时升级更新。

针对 CVE-2021-3711，升级到 OpenSSL 1.1.1l 或更高版本。

针对 CVE-2021-3712，升级到 OpenSSL 1.1.1j、OpenSSL 1.0.2za 或更高版本。

下载链接：

https://www.openssl.org/source/

补丁链接：

CVE-2021-3711（OpenSSL 1.1.1l）：

https://github.com/openssl/openssl/commit/59f5e75f3bced8fc0e130d72a3f582cf7b480b46

CVE-2021-3712（OpenSSL 1.1.1j）：

https://github.com/openssl/openssl/commit/94d23fcff9b2a7a8368dfe52214d5c2569882c11

CVE-2021-3712（OpenSSL 1.0.2za）：

https://github.com/openssl/openssl/commit/ccb0a11145ee72b042d10593a64eaf9e8a55ec12

下载链接：

https://www.openssl.org/news/vulnerabilities.html#CVE-2021-3711

https://securityaffairs.co/wordpress/121426/hacking/cve-2021-3711-openssl-flaws.html?

https://nvd.nist.gov/vuln/detail/CVE-2021-3711

2. F5 8 月多个安全漏洞

漏洞概述

2021 年 8 月 24 日，F5 发布安全更新，修复了其 BIG-IP 等产品中的 29 个安全漏洞。这些漏洞包括经过身份验证的远程命令执行、XSS、CSRF、SSRF 和拒绝服务等。

漏洞详情

本次修复的高危漏洞为 13 个，除 CVE-2021-23031 之外，其它漏洞的 CVSS 评分范围为 7.2-7.5，5 个漏洞影响了 WAF 和 ASM，1 个漏洞影响了 DNS 模块。

其中包括一个在特定条件下被利用时评级为严重的漏洞，该漏洞的 CVE 编号为 CVE-2021-23031，是 BIG-IP Web 应用防火墙（WAF）和应用安全管理器（ASM）流量管理用户界面（TMUI）上的权限提升漏洞。该漏洞的 CVSS 评分为 8.8，经过身份验证且具有配置实用程序访问权限的攻击者可以利用此漏洞来提升权限，最终可以执行任意系统命令、创建或删除任意文件、禁用服务等。但如果应用了设备模式，该漏洞的 CVSS 评分将提升为 9.9。

F5 本次发布的安全更新中的 13 个高危漏洞及其影响范围、修复版本如下:

CVE ID	严重性	CVSS评分	受影响产品	受影响版本	修复版本
CVE-2021-23025	高	7.2	BIG-IP (所有模块)	15.0.0 - 15.1.0 14.1.0 - 14.1.3 13.1.0 - 13.1.3 12.1.0 - 12.1.6 11.6.1 - 11.6.5	16.0.0 15.1.0.5 14.1.3.1 13.1.3.5
CVE-2021-23026	高	7.5	BIG-IP (所有模块)	16.0.0 - 16.0.1 15.1.0 - 15.1.2 14.1.0 - 14.1.4 13.1.0 - 13.1.4 12.1.0 - 12.1.6 11.6.1 - 11.6.5	16.1.0 16.0.1.2 15.1.3 14.1.4.2 13.1.4.1
			BIG-IQ	8.0.0 - 8.1.0 7.0.0 - 7.1.0 6.0.0 - 6.1.0	无
CVE-2021-23027	高	7.5	BIG-IP (所有模块)	16.0.0 - 16.0.1 15.1.0 - 15.1.2 14.1.0 - 14.1.4	16.1.0 16.0.1.2 15.1.3.1

					14.1.4.3
CVE-2021-23028	高	7.5	BIG-IP (WAF、ASM)	16.0.1 15.1.1 - 15.1.3 14.1.3.1 - 14.1.4.1 13.1.3.5 - 13.1.3.6	16.1.0 16.0.1.2 15.1.3.1 14.1.4.2 13.1.4
CVE-2021-23029	高	7.5	BIG-IP (WAF、ASM)	16.0.0 - 16.0.1	16.1.0 16.0.1.2
CVE-2021-23030	高	7.5	BIG-IP (WAF、ASM)	16.0.0 - 16.0.1 15.1.0 - 15.1.3 14.1.0 - 14.1.4 13.1.0 - 13.1.4 12.1.0 - 12.1.6	16.1.0 16.0.1.2 15.1.3.1 14.1.4.3 13.1.4.1
CVE-2021-23031	高/严重（仅	8.8/9.9	BIG-IP (WAF、	16.0.0 - 16.0.1 15.1.0 - 15.1.2 14.1.0 - 14.1.4	16.1.0 16.0.1.2 15.1.3

	设备模式)		ASM)	13.1.0 - 13.1.3 12.1.0 - 12.1.5 11.6.1 - 11.6.5	14.1.4.1 13.1.4 12.1.6 11.6.5.3
CVE-2021-23032	高	7.5	BIG-IP (DNS)	16.0.0 - 16.0.1 15.1.0 - 15.1.3 14.1.0 - 14.1.4 13.1.0 - 13.1.4 12.1.0 - 12.1.6	16.1.0 15.1.3.1 14.1.4.4
CVE-2021-23033	高	7.5	BIG-IP (WAF、ASM)	16.0.0 - 16.0.1 15.1.0 - 15.1.3 14.1.0 - 14.1.4 13.1.0 - 13.1.4 12.1.0 - 12.1.6	16.1.0 15.1.3.1 14.1.4.3 13.1.4.1
CVE-2021-23034	高	7.5	BIG-IP	16.0.0 - 16.0.1 15.1.0 - 15.1.3	16.1.0 15.1.3.1
CVE-2021-23035	高	7.5	BIG-IP	14.1.0 - 14.1.4	14.1.4.4
CVE-2021-23036	高	7.5	BIG-IP (WAF	16.0.0 - 16.0.1	16.1.0 16.0.1.2

			、ASM、DataSafe)		
CVE-2021-23037	高	7.5	BIG-IP	16.0.0 - 16.1.0 15.1.0 - 15.1.3 14.1.0 - 14.1.4 13.1.0 - 13.1.4 12.1.0 - 12.1.6 11.6.1 - 11.6.5	无

此外，F5 还修复了其 BIG-IP 等产品中的其它 16 个中危和低危漏洞，这些漏洞的 CVSS 评分范围为 3.7-6.8，攻击者可以利用这些漏洞执行 XSS 攻击、SQL 注入、访问任意文件等。

安全建议

目前这些漏洞已在部分版本中修复，F5 建议客户将 BIG-IP 设备至少更新或升级到 BIG-IP 14.1.0，将 BIG-IP VE 至少更新或升级到 BIG-IP 15.1.0，建议参考官方公告及时升级更新。

下载链接：

https://support.f5.com/csp/article/K50974556

参考链接：

https://support.f5.com/csp/article/K50974556

https://www.bleepingcomputer.com/news/security/critical-f5-big-ip-bug-impacts-customers-in-sensitive-sectors/

https://securityaffairs.co/wordpress/121454/security/f5-big-ip-critical-flaw.html?

0x02 本周安全态势

1. 勒索软件 LockFile 利用 ProxyShell 和 PetitPotam 漏洞劫持 Windows 域

风险概述

2021 年 08 月 21 日，CISA 发布紧急通告，恶意网络攻击者正在积极利用 ProxyShell 漏洞，成功利用这些漏洞的攻击者可以在易受攻击的系统上执行任意代码，以及在受感染系统上放置后门或部署恶意软件，如勒索软件 LockFile。赛门铁克表示，一旦在受影响系统上立足，LockFile 团伙就会通过 PetitPotam 漏洞攻击域控制器，从而控制 Windows 域。

攻击详情

ProxyShell 漏洞是以下三个 Microsoft Exchange 漏洞的统称，它们能够导致未经身份验证的远程代码执行：

- CVE-2021-34473 ：预授权路径混淆导致 ACL 绕过(已于 4 月通过 KB5001779 修复）。
- CVE-2021-34523：Exchange PowerShell 后端权限提升（已于 4 月通过 KB5001779 修复）。
- CVE-2021-31207：身份验证后的任意文件写入导致 RCE（已于 5 月通过 KB5003435 修复）。

近日，恶意攻击者正在积极利用 ProxyShell 漏洞扫描和入侵 Microsoft Exchange 服务器，以投放恶意 webshell。研究人员表示，自 ProxyShell 漏洞的 PoC 公开以来，至少在 1900 个未打补丁的 Exchange 服务器中检测到了 140 多个 webshell。目前，研究人员已经确定了名为 LockFile 的新勒索软件团伙正在积极利用 ProxyShell 漏洞入侵 Microsoft Exchange 服务器。

根据赛门铁克的分析，LockFile 勒索软件团伙最初是通过 Microsoft Exchange Server 获得对受害者网络的访问权限，然后利用 PetitPotam 漏洞来接管域控制器，最终控制 Windows 域。

LockFile 勒索软件于 7 月被首次发现，其攻击对象主要集中在美国和亚洲，受害者涉

及金融服务、制造、工程、法律、商业服务、旅行和旅游等行业的组织。赛门铁克在其分析文章中表示，LockFile 勒索软件的赎金通知与 LockBit 勒索软件团伙使用的赎金通知非常相似，并且其联系电子邮件地址还涉及到了 Conti 团伙。加密文件时，勒索软件会在加密文件的名称后加上.lockfile 扩展名。

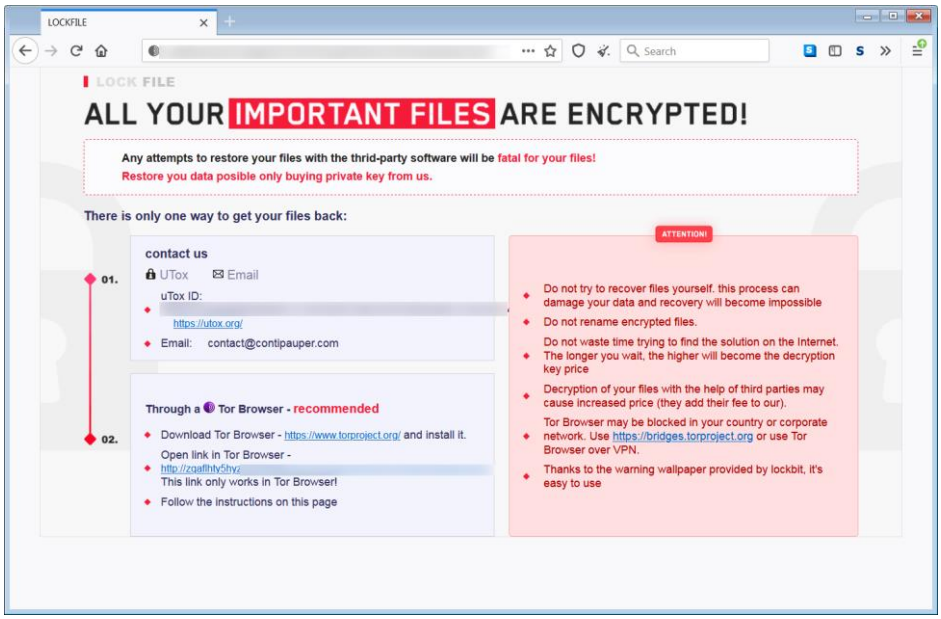

图 1. LockFile 赎金记录

根据对 LockFile 的攻击链的分析，研究人员表示，在入侵受害者的 Exchange 服务器时，攻击者会运行 PowerShell 命令，从远程位置下载文件。在攻击的最后阶段（即部署勒索软件前 20 到 30 分钟），攻击者通过在受感染的 Exchange 服务器上安装 PetitPotam 漏洞和两个文件控制域控制器：

- Active_desktop_render.dll
- active_desktop_launcher.exe（合法的 KuGou Active Desktop 启动器）

其中，exe 文件用于 DLL 搜索顺序加载攻击以加载恶意的 active_desktop_render.dll 文件。当 active_desktop_render.dll 文件被 active_desktop_launcher.exe 加载时，将试图加载和解密本地目录中一个名为 desktop.ini 的文件。如果该文件被成功加载和解密，

该文件中的 shellcode 将被执行。该 shellcode 很可能会激活利用 PetitPotam 漏洞的 efspotato.exe 文件。PetitPotam 漏洞是一个 NTLM 中继攻击漏洞，可被低权限的攻击者用来接管域控制器。

一旦获得对本地域控制器的访问权，攻击者就会将 LockFile 勒索软件连同批处理文件和支持的可执行文件复制到域控制器上的"sysvol/domain/scripts "目录，该目录用于当网络客户认证到域控制器时向他们部署脚本。这意味着，当这些恶意文件被复制过来之后，任何客户在认证到域的时候都会执行这些文件。

风险等级

严重。

攻击者可利用这些漏洞安装 webshell 或者控制 Windows 域。

影响范围

ProxyShell 漏洞（CVE-2021-34473、CVE-2021-34523 和 CVE-2021-31207）和 PetitPotam 漏洞（CVE-2021-36942、ADV210003）的影响范围请参考微软官方公告。

安全建议

鉴于勒索软件 LockFile 同时利用 Microsoft Exchange ProxyShell 漏洞和 Windows PetitPotam NTLM Relay 漏洞，因此建议 Windows 管理员尽快应用安全更新并对 Exchange 服务器创建离线备份。

- 针对 ProxyShell 漏洞，安装最新的 Microsoft Exchange 累积更新。下载链接：https://docs.microsoft.com/en-us/exchange/new-features/build-

numbers-and-release-dates?view=exchserver-2019

- Windows PetitPotam 攻击目前微软官方暂未完全修复，可以使用 0patch 的非官方补丁来阻止此 NTLM 中继攻击，或者应用 NETSH RPC 过滤器，阻止对 MS-EFSRPC API 中的脆弱功能的访问。

  0patch 链接：https://0patch.com/

  NETSH RPC 过滤器链接：

  https://www.bleepingcomputer.com/news/microsoft/windows-petitpotam-attacks-can-be-blocked-using-new-method/

可以使用以下查询来检查 Microsoft Exchange 服务器是否已被扫描过 ProxyShell 漏洞。

```
W3CIISLog
| where csUriStem == "/autodiscover/autodiscover.json"
| where csUriQuery has "PowerShell" | where csMethod == "POST"
```

通用安全建议

- 及时安装补丁，定期更新软件、程序和应用程序，确保应用程序是最新的，以保护系统免受漏洞利用。
- 加强系统和网络的访问控制，修改防火墙策略，关闭非必要的应用端口或服务，减少将危险服务（如 SSH、RDP 等）暴露到公网，以减少攻击面。
- 预防 0day 漏洞和恶意软件，安全产品实时更新最新规则或相关防护指标。

- 加强系统用户和权限管理，启用多因素认证机制和最小权限原则，用户和软件权限应保持在最低限度。
- 启用强密码策略并设置为定期修改。
- 使用最新、全面的威胁情报信息，监控网络和安全事件，以快速响应攻击。

参考链接：

https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows

https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-being-hacked-by-new-lockfile-ransomware/

https://www.bleepingcomputer.com/news/security/lockfile-ransomware-uses-petitpotam-attack-to-hijack-windows-domains/

https://thehackernews.com/2021/08/microsoft-exchange-under-attack-with.html

2. 2021 年上半年针对 Linux 的常用漏洞 TOP15

风险概述

2021 年 08 月 23 日，趋势科技发布了 2021 年上半年的 Linux 威胁报告，公开披露了针对 Linux 系统的恶意软件和被攻击者利用数百万次入侵 Linux 系统的前 15 个漏洞，以及最流行的 15 个 Docker 镜像中的数百个漏洞。

攻击详情

Linux 是一种独特的操作系统，其因具有稳定性、灵活性和开源特性而被广泛使用。

根据趋势科技的研究，在 2021 年 7 月，发现近 1400 万个基于 Linux 的系统直接暴露在 Internet 上，这使它们成为网络攻击者的有利目标，并最终被部署恶意 web shell、挖矿软件、勒索软件和其它木马等。在趋势科技检测到的近 1300 万个针对基于 Linux 的云环境的恶意软件事件中，挖矿软件和勒索软件占所有恶意软件的 24%和 11%，Webshell 占 19%。

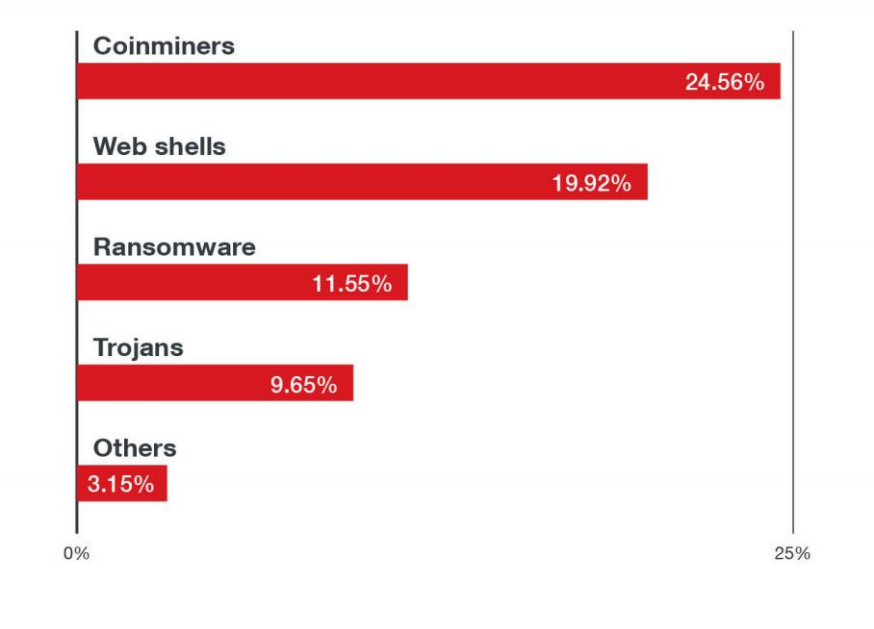

图 1.2021 年上半年在 Linux 系统中发现的主要威胁类型

值得注意的是，挖矿软件的流行率很高，其中 Coinminer.Linux.MALXMR.SMDSL64 和 Coinminer.Linux.MALXMR.PUWELQ 是最为普遍的家族；至于 webshell，其中检测到的最多的家族是 Backdoor.PHP.WEBSHELL.SBJKRW、Backdoor.PHP.WEBSHELL.SMMR 和 Backdoor.PHP.WEBSHELL.SMIC。 鉴于云计算的计算能力，攻击者将窃取资源以进行挖矿活动作为明确动机。此外，挖矿活动近年来还一直困扰着容器环境。勒索软件是一种普遍的 Linux 威胁，根据我们的数据，DoppelPaymer，一个利用双重勒索战术的现代勒索软件家族是最常见的勒索软件家族。在我们对勒索软件的监测中，我们最近还发现了其它针对 Linux 系统的勒索软件变种，如 RansomExx、DarkRadiation 或 DarkSide。

上述恶意软件家族针对的基于 Linux 的前四个发行版为：

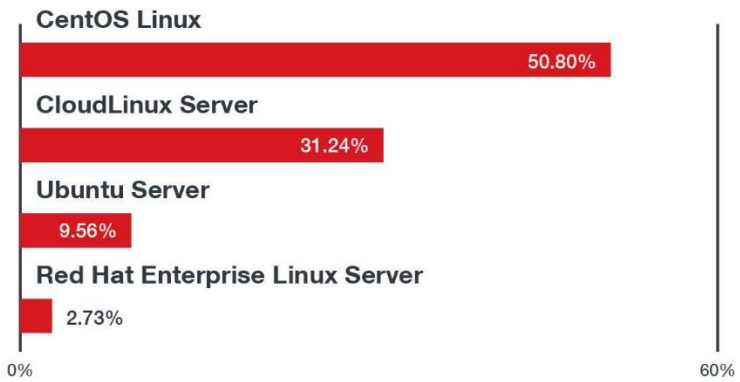

图 2.受影响的主要 Linux 发行版

此外，通过分析 2021 年上半年中 100,000 个独特 Linux 主机报告的超过 5000 万个事件，研究人员观察到了被积极利用或 PoC/EXP 公开的大约 200 个不同的漏洞，其中前 15 个漏洞如下：

- CVE-2017-5638 ：Apache Struts 2 远程代码执行 (RCE) 漏洞(CVSS 评分：10.0)

- CVE-2017-9805 ： Apache Struts 2 REST plugin XStream RCE 漏洞(CVSS 评分：8.1)
- CVE-2018-7600 ： Drupal Core RCE 漏洞(CVSS 评分：9.8)
- CVE-2020-14750 ： Oracle WebLogic Server RCE 漏洞(CVSS 评分：9.8)
- CVE-2020-25213 ： WordPress 文件管理器 plugin RCE 漏洞(CVSS 评分：10.0)
- CVE-2020-17496 ： vBulletin 'subwidgetConfig' 未经身份验证的 RCE 漏洞(CVSS 评分: 9.8)
- CVE-2020-11651 ： SaltStack Salt 授权弱点漏洞(CVSS 评分: 9.8)
- CVE-2017-12611 ： Apache Struts OGNL 表达式 RCE 漏洞(CVSS 评分: 9.8)
- CVE-2017-7657 ： Eclipse Jetty 块长度解析整数溢出漏洞(CVSS 评分：9.8)
- CVE-2021-29441 ： Alibaba Nacos AuthFilter 认证绕过漏洞(CVSS 评分: 9.8)
- CVE-2020-14179 ： Atlassian Jira 信息泄露漏洞(CVSS 评分：5.3)
- CVE-2013-4547 ： Nginx 制作的 URI 字符串处理访问限制绕过漏洞(CVSS 评分：8.0)
- CVE-2019-0230 ： Apache Struts 2 RCE 漏洞(CVSS 评分：9.8)
- CVE-2018-11776 ： Apache Struts OGNL 表达式 RCE 漏洞(CVSS 评分：8.1)
- CVE-2020-7961 ： Liferay Portal 不受信任的反序列化漏洞(CVSS 评分：9.8)

最常触发漏洞的应用程序的比例如下：

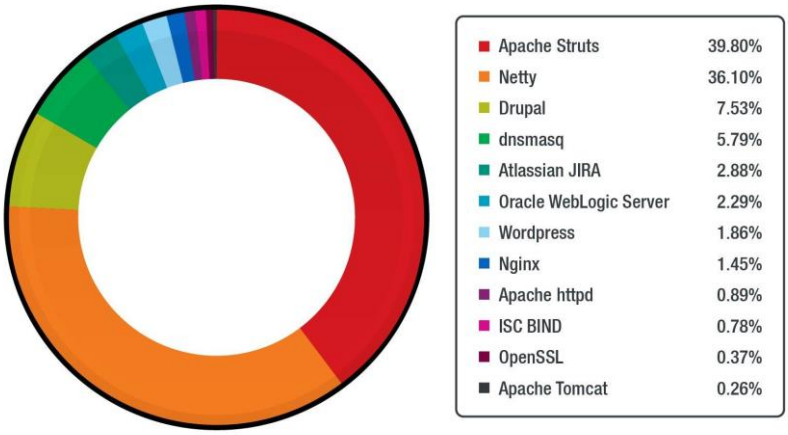

图 3.主要受影响应用程序所占比例

此外，容器是 Linux 生态系统的重要组成部分，同时它也是攻击者的主要目标之一。

下表显示了 Docker Hub 上 15 个最受欢迎的官方 Docker 镜像的漏洞。

Image	漏洞总数	严重	高危	中危	低危	其它
python	482	32	129	246	38	37
node	470	32	126	238	37	37
wordpress	402	26	109	198	40	29
golang	288	10	87	157	13	21
nginx	118	18	41	44	7	8
postgres	86	8	32	35	6	5

Image	漏洞总数	严重	高危	中危	低危	其它
influxdb	85	8	33	34	6	4
httpd	84	7	33	32	6	6
mysql	76	9	28	31	5	3
debian	66	7	26	25	5	3
memcached	65	7	25	25	5	3
redis	65	7	25	25	5	3
mongo	47	3	18	23	3	0
centos	68	7	36	23	2	0
rabbitmq	30	1	7	20	2	0

表 1.15 个最流行的 Docker 镜像以及每个镜像的漏洞数量和级别

风险等级

严重。

攻击者可以利用这些漏洞远程执行代码、部署恶意 webshell、挖矿软件、勒索软件或其它木马等。

影响范围

漏洞的具体影响范围及修复方式请参考官方发布的安全公告。

安全建议

用户和组织应始终应用安全最佳实践，包括使用安全设计方法、部署多层虚拟补丁或漏洞屏蔽、采用最小特权原则以及遵守责任共担模式，建议应用以下措施：

- 使用轻量级基础镜像，如 Alpine Linux。
- 应用最小特权原则，不要以 root 或特权模式运行容器。
- 对容器镜像进行签名和验证，以保护它们免受供应链攻击。
- 主动扫描并修复容器依赖中的漏洞。
- 不要在容器映像上硬编码机密或凭据。

参考链接：

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-threat-report-2021-1h-linux-threats-in-the-cloud-and-security-recommendations#C02

https://thehackernews.com/2021/08/top-15-vulnerabilities-attackers.html

3. Cinobi 银行木马活动分析

概述

在之前的一篇文章中，我们报告了一个称之为 "Operation Overtrap"的活动，该活动以日本为目标，并使用了一种名为 Cinobi 的新型银行木马。这个活动是由我们命名为 "Water Kappa "的组织发起的，它通过垃圾邮件分发 Cinobi。它还使用 Bottle 漏洞工具包传递木马,其中包括较新的Internet Explorer漏洞CVE-2020-1380和CVE-2021-26411，并将其用于恶意广告攻击（仅分发给 Internet Explorer 用户）。在 2020 年和 2021 年上半年，我们观察到 Bottle 漏洞工具包的活动，但 6 月中旬流量减少,这可能表明该组织正在转向新的工具和技术。

同时，我们发现了一个针对日本的基于社会工程的新恶意广告活动，该活动提供了伪装成免费色情游戏、奖励积分应用程序或视频流应用程序的恶意应用程序。该恶意应用程序滥用旁加载漏洞来加载和启动 Cinobi 银行木马。我们认为这是 Water Kappa 的一个新活动，针对的是除 IE 以外的网络浏览器用户。

通过研究 Cinobi 样本，我们发现其整体功能相对保持不变，但配置已经更新，将几个

日本加密货币交易所网站作为目标列表的一部分。该团伙开始使用 Cinobi 窃取其受害者的加密货币账户的凭证。

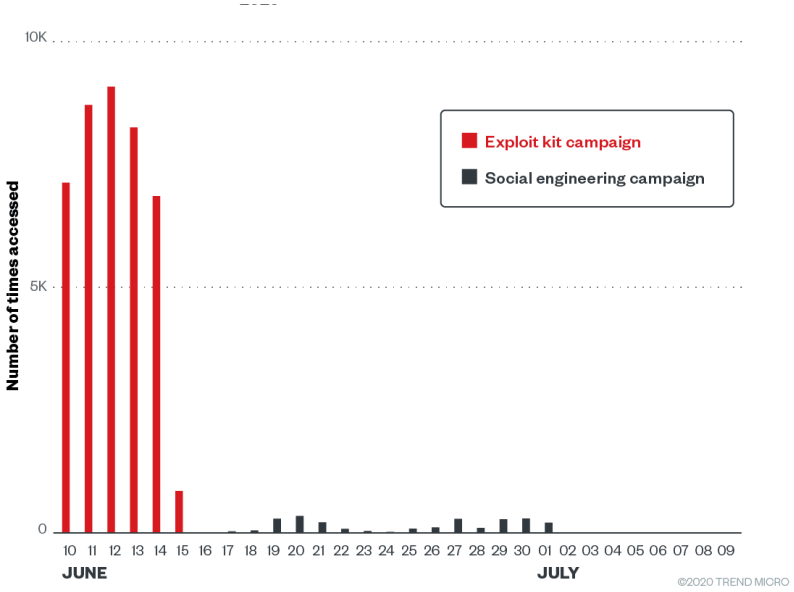

图 1. Water Kappa 活动的时间线

感染过程

该活动的感染程序始于用户收到的恶意广告，这些广告被伪装成日本动画色情游戏、奖励积分应用程序或视频流应用程序的广告。虽然我们观察到他们的恶意广告有五种不同的主题，但他们都试图欺骗受害者使用相同的恶意软件下载相同的压缩包。

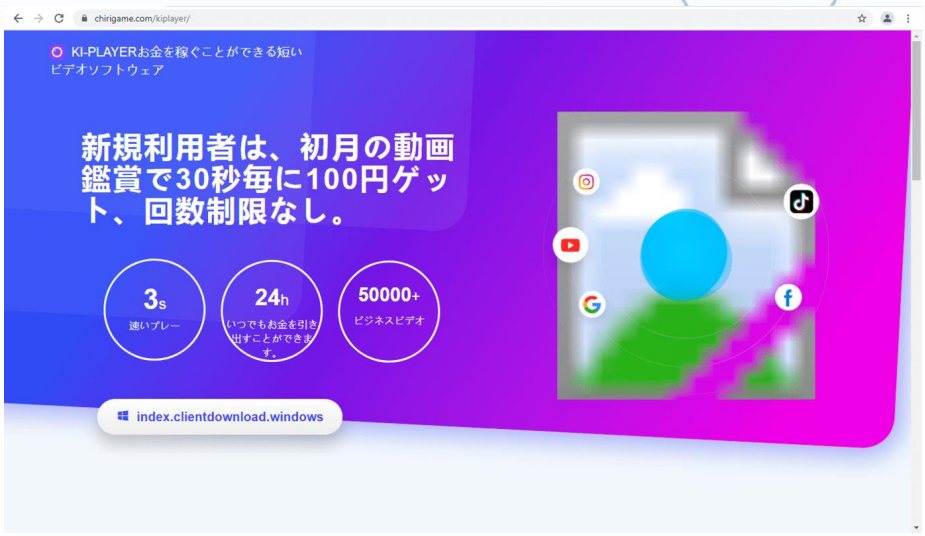

图 2. 伪装成流媒体应用程序下载恶意压缩包的登陆页面

这些恶意广告很可能是由恶意行为者从合法网站克隆的。然后进行小的修改，如删除一些按钮和改变某些信息部分。唯一留下的按钮通向由恶意行为者创建的新页面,该页面指示受害者如何下载和执行应用程序。

点击带有 "index.clientdownload.windows "文字的按钮后（如图 2 所示），登陆页面开始下载 ZIP 包，随后是指导受害者如何打开、提取和执行主要可执行文件。其它四个恶意广告在视觉上看起来不同，但它们的行为和登陆页面是相似的。

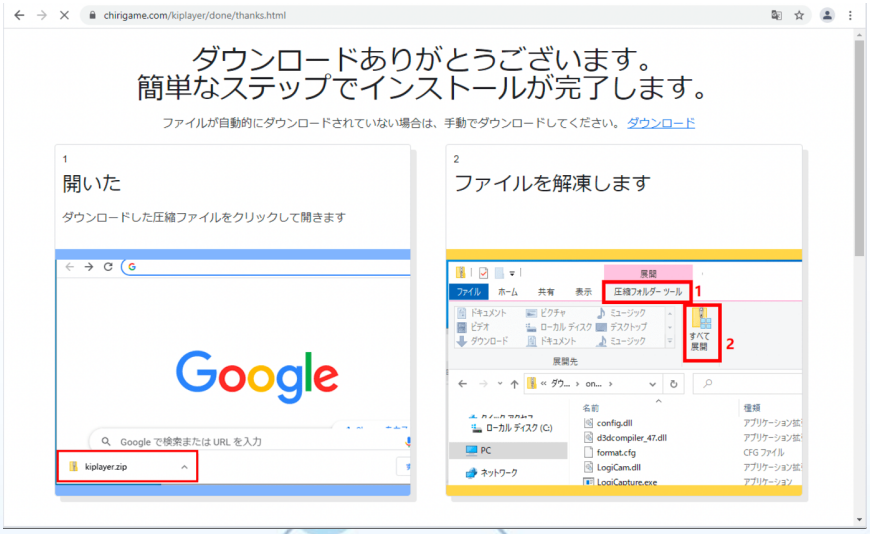

图 3. 执行流应用程序的说明

值得注意的是，对网站的访问是根据 IP 地址来过滤的。非日本的 IP 地址将看到 Cloudflare 的以下错误信息。

图 4. 从非日本 IP 地址访问应用程序或游戏网站时显示的错误

恶意软件分析

解压缩 ZIP 包后，我们注意到图 5 中的列表。其中,我们认为足够有趣且能提供分析的文件用红色标记。

[cef3_2987]		<DIR>	07/28/2021 19:51
avcodec-55	dll	11,681,944	10/19/2018 22:22
avdevice-55	dll	124,040	10/19/2018 22:22
avfilter-4	dll	789,128	10/19/2018 22:22
avformat-55	dll	1,698,952	10/19/2018 22:22
avutil-52	dll	345,736	10/19/2018 22:22
cfg	config	15,895	07/09/2021 15:08
config	dll	34,304	07/09/2021 15:08
d3dcompiler_47	dll	3,466,856	08/27/2018 23:06
format	cfg	1,050	07/09/2021 15:07
LogiCam	dll	358,024	10/19/2018 22:22
LogiCapture	exe	4,287,624	10/19/2018 22:22
LogiCapture.exe	config	18,899	06/21/2021 21:46
LogiCapture.exe	manifest	2,015	08/27/2018 23:06
Native.LogiCapture.exe	manifest	51,703	08/27/2018 23:06
openh264-1.5.0-win32msvc	dll	619,008	06/21/2021 21:03
swresample-0	dll	104,072	10/19/2018 22:22
swscale-2	dll	448,136	10/19/2018 22:22
VHMediaCOM	dll	4,402,312	10/19/2018 22:22
Xjs	dll	34,304	07/09/2021 15:07
XjsEx	dll	454,280	10/19/2018 22:22

图 5. ZIP 包的内容,恶意文件用红色标记

其中,大多数文件是从旧版本的“Logitech Capture”应用程序中提取的合法文件，日期为 2018 年。合法且已签名的 LogiCapture.exe(08FB68EB741BF68F3CFC29A4AD3033D75AD57798ED826D926344015BDB8B0EBB)应用程序在 LogiCapture.exe.config 中通过自定义应用程序设置被指示加载 Xjs.dll 库。Xjs.dll 加载 format.cfg 文件，解密 shellcode，并执行它。

图 6. 加密后的 format.cfg shellcode

图 7. 加密后的 format.cfg shellcode

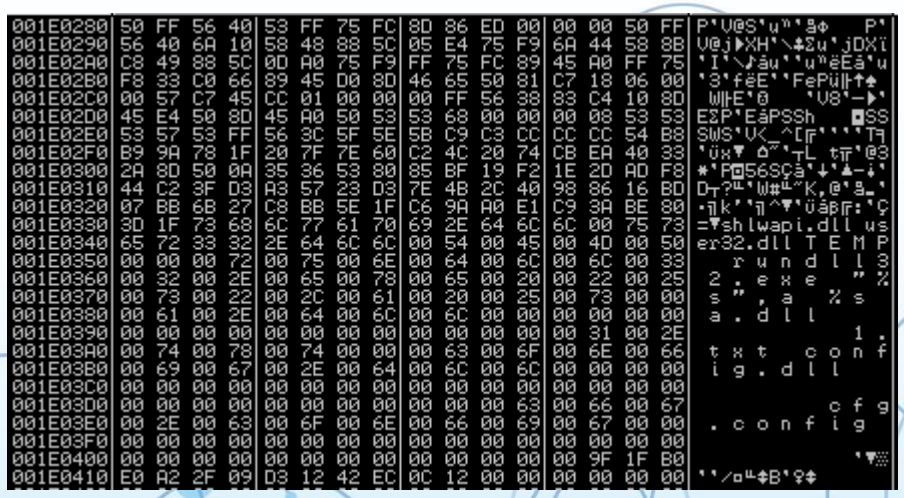

图 8. 解密后的 format.cfg shellcode,带有文件名和 rundll32 命令的字符串是可见的

嵌入到 format.cfg 的 shellcode 将 config.dll 和 cfg.config 复制到临时目录%TEMP%，将这些文件重命名为 a.dll 和 1.txt，并通过以下命令执行 a.dll 库中名为 "a "的导出函数：

```
rundll32.exe "%TEMP%\a.dll",a%TEMP%\1.txt
```

Config.dll（重命名为 a.dll）解析必要的 API，加载 cfg.config（重命名为 1.txt）的内容，使用 XOR 密钥对其进行解密，并执行 shellcode。解密后的 cfg.config 是 Cinobi 银行木马的第一阶段（正如我们在 2020 年的文章中所述）。

```
7368100C   8B45 08          MOV EAX,DWORD PTR SS:[EBP+8]
7368100F   8D0C06          LEA ECX,[EAX+ESI]
73681012   33D2            XOR EDX,EDX
73681014   6A 09           PUSH 9
73681016   8BC6            MOV EAX,ESI
73681018   5F              POP EDI
73681019   F7F7            DIV EDI
7368101B   8A82 EC8C6873   MOV AL,BYTE PTR DS:[EDX+73688CFC]      ASCII "hQ6Bd03wb"
73681021   3001            XOR BYTE PTR DS:[ECX],AL
73681023   46              INC ESI
73681024   3B75 0C         CMP ESI,DWORD PTR SS:[EBP+0C]
73681027 ^ 72 E3           JB SHORT 7368100C
```

图 9. config.dll 中解密 cfg.config shellcode 的例程

```
7368112C   57              PUSH EDI
7368112D   FF35 788B6873    PUSH DWORD PTR DS:[73688B78]
73681133   A3 5E8C6873      MOV DWORD PTR DS:[73688C5E],EAX
73681138   891D 9F8B6873    MOV DWORD PTR DS:[73688B9F],EBX
7368113E   890D A38B6873    MOV DWORD PTR DS:[73688BA3],ECX
73681144   FFD0              CALL EAX                              kernel32.EnumUILanguagesA
```

图 10. Config.dll 中的调用指令执行解密后的 cfg.config shellcode

Cinobi 银行木马分为四个阶段，每个阶段都会下载额外的组件，并可能进行环境或反虚拟机（VM）检查。有两个命令和控制（C&C）服务器，其中一个返回第 2 至第 4 阶段，而另一个返回配置文件。

恶意行为者在 2021 年夏天变得更加活跃,我们注意到还有几个版本，与之前描述的版

本略有不同。除了添加了四个恶意文件的应用程序包（如图 5 所示）之外，我们还注意到一个只有三个文件 (xjs.dll、format.cfg 和一个名为 "ros "的文件) 的重构版，只有三个阶段，以及一个提供配置文件的 C&C 服务器。

在重构后的版本中，Xjs.dll 解密并加载 format.cfg，这是 Cinobi banker 的第一阶段。这个阶段，与我们去年文章中所述不同，并没有从第一个 C&C 服务器下载 Tor 和其它附加阶段。相反，它从名为 "ros "的文件中读取和提取文件，ros 文件是一个包含第二阶段和第三阶段的加密包、一个包含 C&C 服务器的配置文件以及一个带有 Tor 的存档。

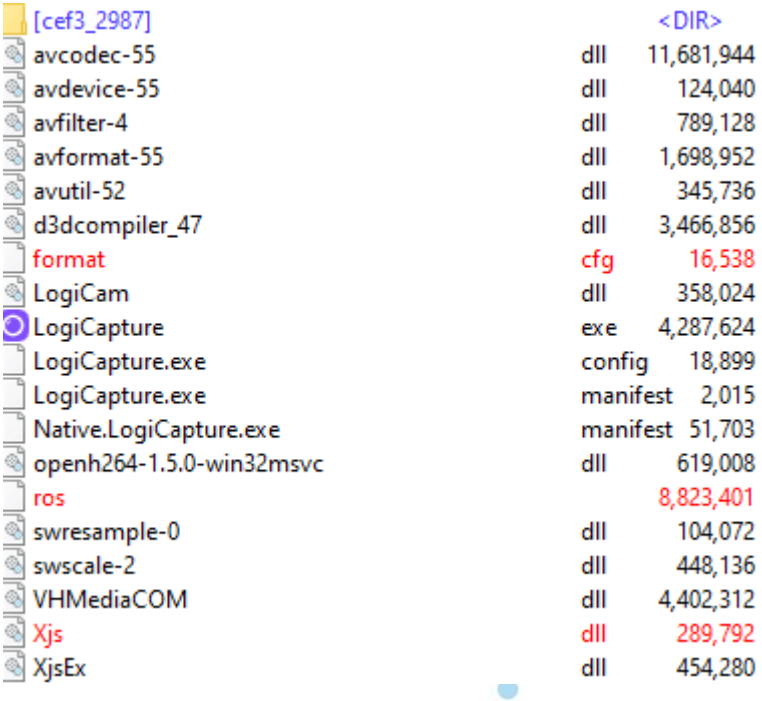

图 11：重构后的 Cinobi banker

其中最重要的是 form-grabbing 功能所针对的网站的配置文件。在撰写本文时，我们注意到，该银行木马的目标是 11 家日本金融机构的用户，其中至少有三家涉及加密货币交易。

当受害者访问配置文件中提到的网站之一，并将填好的表格发回服务器时，该恶意软件

的 form-grabbing 功能就会被激活。在下图中，我们展示了填充数据的登录表单示例。

点击提交按钮后，一个带有加密请求的文本文件会短暂出现在安装了银行木马的文件夹中，解密临时创建的文本文件后，可以看到突出显示的被盗凭证。

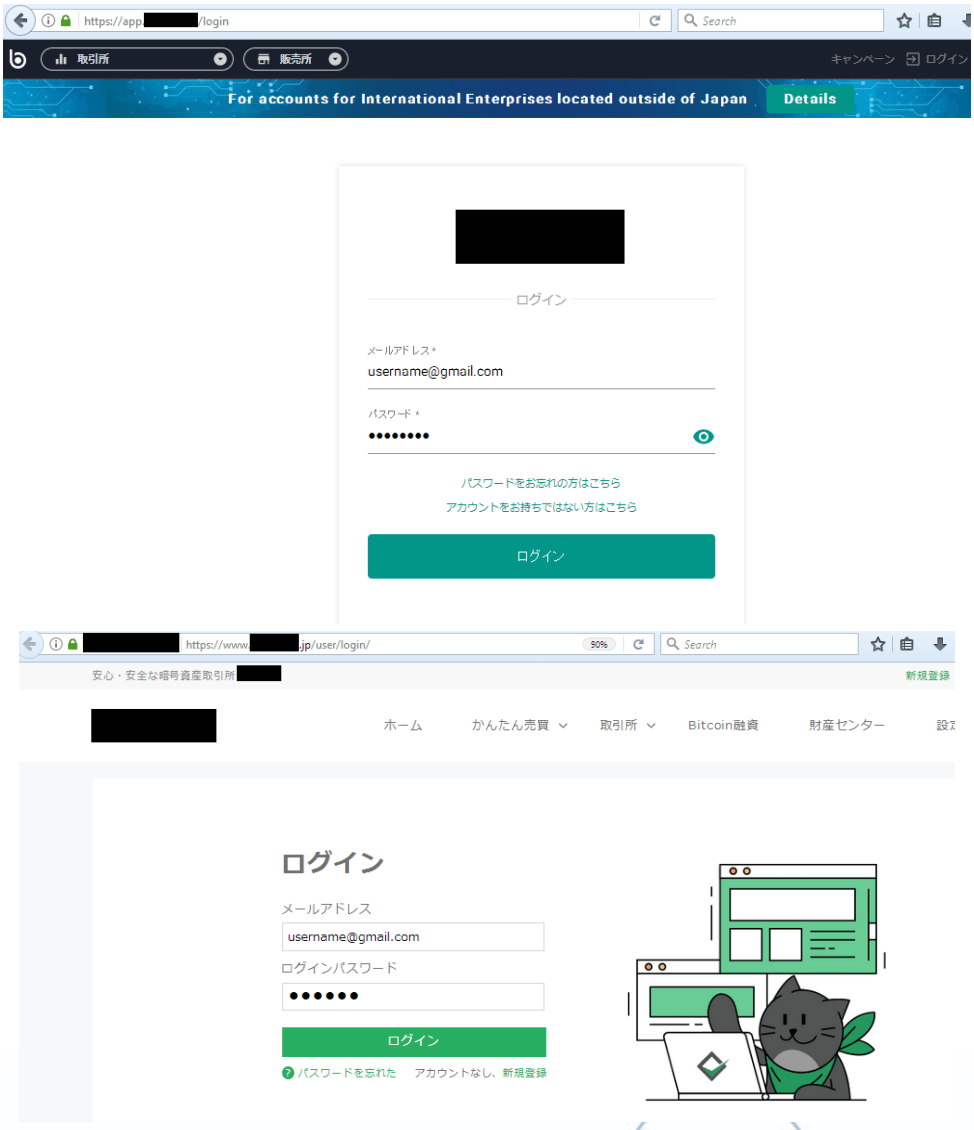

图 12. 处理加密货币的公司的目标网站

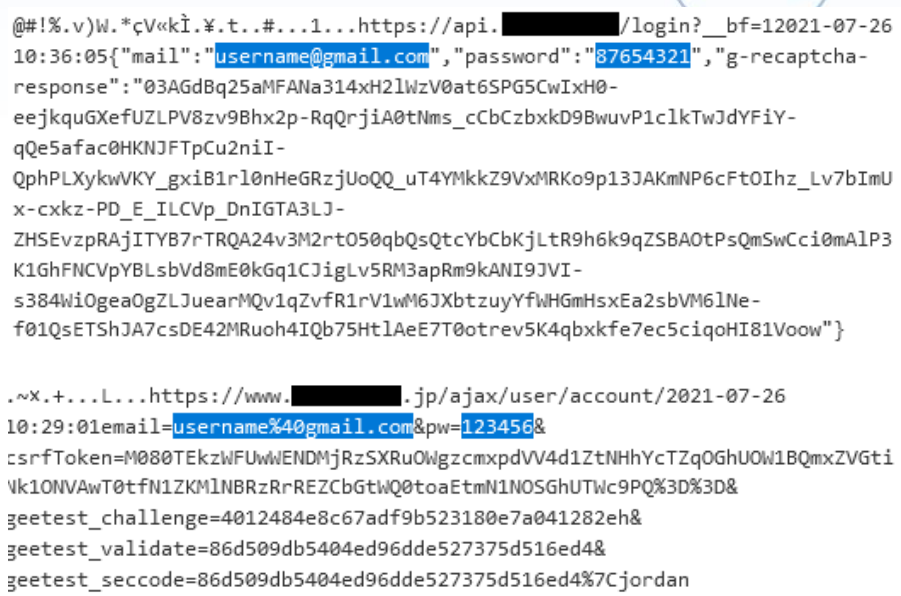

图 13. 解密的请求,登录凭证以蓝色突出显示

结论

新的恶意广告活动表明，Water Kappa 仍然活跃，并不断发展他们的工具和技术，以获得更大的经济利益，当然，他们此次活动的目的也是为了窃取加密货币。为了降低被感染的风险，用户需要警惕网站上的可疑广告，并尽可能只从可信的来源下载应用程序。

提供多层防御系统的解决方案可以通过检测、扫描和阻止恶意 URL，帮助企业保护其员工免受此类活动的影响。

IoC

SHA256

SHA256	文件名	说明	分析

124FE26D53E2702B42AE07F8AEC5EE4E79E7424BCE6ECDA608536BBF0A7A2377	oneroom_setup.zip	Malicious game archive	Trojan.Win32.SHELLOAD.AZ
E667F9C109E20900CC8BADD09EDE6CDCE0BDC77164CFD035ACE95498E90D45E7	oneroom_game.zip	Malicious game archive	Trojan.Win32.SHELLOAD.AZ
93FFE7CF56FEB3FB541AEF91D3FC04A5CF22DF428DC0B7E5FEB8EDDDC2C72699	Magicalgirl.zip	Malicious game archive	Trojan.Win32.SHELLOAD.AZ
AD13BB18465D259ACC6E4CEBA24BEFF42D50843C8FD92633C569E493A075FDDC	kiplayer.zip	Malicious streaming archive	Trojan.Win32.SHELLOAD.BA
A9EF18B012BD20945BB3533DEEC69D82437BF0117F83B2E9F9E7FACC5AA81255	oneroom_game_v7.zip	Malicious game archive	Trojan.Win32.SHELLOAD.AZ
6C1F4FFA63EE7094573B0F6D1BD51255F603BC8958757405C8C998416537D587	Xjs.dll	First shellcode loader	Trojan.Win32.SHELLOAD.AZ
1366E2AC6365E4B76595A19760438D876E01DB40C60EC3F42849F0218B724F1B	Xjs.dll	First shellcode loader	Trojan.Win32.SHELLOAD.AZ

0B3E5E2406490DF17A198A8340B103BB331A5277461234F3F90ED257E418C1F8	Xjs.dll	First shellcode loader	Trojan.Win32.SHELLOAD.AZ
3E0FAEE93F6EF572537735C7F2D82D151C5A21EB30EACC576B3B66320C74FD34	format.cfg	Encrypted shellcode	Trojan.Win32.SHELLOAD.AZ.enc
DB6CBE4EE82F87008B34D1D4E9AA6EE3C9CCD21CB7A0B60925D5DA8D1295A269	format.cfg	Encrypted shellcode	Trojan.Win32.SHELLOAD.AZ.enc
3B7FB5EC8180AD74871EB9F5B59E6E98A188CE84BA3BD6ADD9B4BCFCCB80C137	format.cfg	Encrypted shellcode	Trojan.Win32.SHELLOAD.AZ.enc
52E2B9CBA4E1BEE1EB3ED9D03BC33EADB6C8D6AAC8598679AA95690E587BE7C4	config.dll	Cinobi 1st stage loader; 32bit	Trojan.Win32.CINOBI.A
F5AD9E32A84DF617ABA3786F19BA7DAB4B4BD8A27627232D3AACE760511AEDF7	config.dll	Cinobi 1st stage loader; 32bit	Trojan.Win32.CINOBI.A
45C7C36E7E8B832815D8B03651EDC14F864B52E1C599E5336A1AAA0BD47FF3E3	cfg.config	Encrypted 1st stage of Cinobi; 32bit	Trojan.Win32.CINOBI.AC

522C59BACE844A3D76B674842373DDBF959FC5B352317B024DBF225F536A641E	cfg.config	Encrypted 1st stage of Cinobi; 32bit	Trojan.Win32.CINOBI.AC
16AB933AD01D73120EE5B764C12057FF7F6DC3063BBC377CDB87419A30532323	N/A	2nd and 3rd stage loader; 32bit	Trojan.Win32.CINOBI.AC
9D10AC2A2C7C58F1E1D4B745746AA5F0CE699C0DB87CCCA43418435FAA03AD1B	N/A	2nd stage encrypted; 32bit	Trojan.Win32.CINOBI.AC.enc
C4039CD7DB24158BE51DA9010E6A367F5253F40F007B656407FB69D279732784	N/A	3nd stage encrypted; 32bit	Trojan.Win32.CINOBI.AC.enc
2A6FE431326ACCAF31EA7CA7CD1214AD5EFCA891619859BCF60671A62C8D81F4	N/A	Cinobi 4th stage (last); 32bit	TrojanSpy.Win32.CINOBI.C
258EDBBAC7E78B4F51433807B237FC0ED7F76031795EA48A4FEFB38949F9B3B6	N/A	2nd and 3rd stage loader; 64bit	Trojan.Win64.CINOBI.AA
A3010F206656752FAD70EF7637947933152E7ADC883B43D0832B2234C8E6F968	N/A	2nd stage encrypted; 64bit	Trojan.Win64.CINOBI.AA.enc

E037839A3DACC3153754A156136E9EAD2F4C52939FE869B3981C4BB5114202C8	N/A	3rd stage encrypted; 64bit	Trojan.Win64.CINOBI.AA.enc
F8B80978D4548139E824863DD661E40AF4C2523C3E93547E4F167A749E108280	N/A	Cinobi 4th stage (last); 64bit	TrojanSpy.Win64.CINOBI.AA
B157BEAC5516D05A014527B3F0FE4B01683CAAC9FFF6608B67A8BA62DF5EF838	N/A	2nd and 3rd stage loader; 32bit	Trojan.Win32.CINOBI.A
2384FDA35A293B5F5B32B09E8DC455E7CE40A92D25CD9BACEEAB494785426B46	N/A	2nd stage encrypted; 32bit	Trojan.Win32.CINOBI.A.enc
9FF65052FE93A884D7BCE36E87F4DE104839F72F26AF66785B2D98EAB706C816	N/A	3nd stage encrypted; 32bit	Trojan.Win32.CINOBI.AC.enc
31C936D08E9BA8FDA86844F67363223BDB6A917F530571ABCB3F584874909FEA	N/A	Cinobi 4th stage (last); 32bit	TrojanSpy.Win32.CINOBI.C
00F24AC0AD19DC3EE05A112F7650AABA16041020263EA851C90F3C0A61C7EC57	N/A	2nd and 3rd stage loader; 64bit	Trojan.Win64.CINOBI.AB
B0E5BB79CDFAD284D88BC	N/A	2nd stage	Trojan.Win64.C

26DB4289A51F114CC71C928E8A9951DC8C498A243B9		encrypted; 64bit	INOBI.AB.enc
095E85EBE2155798FB3A5FBD57196CF377B56FB2176CFF3A776302DCB806237D	N/A	3rd stage encrypted; 64bit	Trojan.Win64.CINOBI.AB.enc
B36BFF265EE47D31E4C70EE78BADCFCC0DE89643DA61C1BF16BA2D6F36A62936	N/A	Cinobi 4th stage (last); 64bit	TrojanSpy.Win64.CINOBI.AB
E41AB2DE9CCFFE3AADDB32C224114D88D2E61C02D52F89829B544F49B672D74D	N/A	2nd stage loader; 32bit	Trojan.Win32.CINOBI.AA
59DF3B32A0D3FEFB15C6AAB7D9254E597484A486156CBC1F403A376A8A0C25FB	N/A	2nd stage encrypted; 32bit	Trojan.Win32.CINOBI.AA.enc
043720F493CA7A2B2E18CCD7AEC8CB8D577F544AAE02975BFE313046E839F107	N/A	2nd stage loader; 64bit	Trojan.Win64.CINOBI.AA
83F7D60D172628E421EF038566F449E8708573201C8F23398F0F06B5F33123DA	N/A	2nd stage encrypted; 64bit	Trojan.Win64.CINOBI.AA.enc
58C60164AAA23777E5A8D	N/A	Cinobi	TrojanSpy.Win

BBA25C4466A5B1ECA54EF8CF02BA2CD1AB7084753BE		3rd stage (last); 32bit	32.CINOBI.B
F3DA0C082EB271A2F0DD54F2A3260BFC02BDF311EBCB1C619D479FCBB1E9F6F5	N/A	Cinobi 3rd stage (last); 64bit	TrojanSpy.Win64.CINOBI.AA

Domain

IP Address/Domain/URL	说明
www[.]chirigame[.]com	Malvertising domain
www[.]supapureigemu[.]com	Malvertising domain
www[.]getkiplayer[.]com	Malvertising domain
www[.]magicalgirlonlive[.]com	Malvertising domain
a7q5adiilsjkujxk[.]onion	Cinobi banker's C&C serving stages 2-4
5lmt6t4kaymuwvm5[.]onion	Cinobi banker's C&C serving configuration files

原文链接:

https://www.trendmicro.com/en_us/research/21/h/cinobi-banking-trojan-

targets-users-of-cryptocurrency-exchanges-.html