金融行业

3 月报
2021 年

安全月报

安全观点 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

安全观点

针对银行业精准短信钓鱼事件
安全分析

行业研究

以蓝军视角跟踪和分析CANVAS
攻击框架泄露事件

Webshell知多少——Webshell威胁分析

公安部：去年抓获侵犯公民个人信息
犯罪嫌疑人9700 余名

被控非法侵犯用户隐私，TikTok
同意支付9200 万美元进行和解

加密货币诈骗盗取1600 万美元

NSFOCUS

贴身服务 加油干

绿盟科技城商行信息安全解决方案

无缝衔接 | 密切配合

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为金融、政府、运营商、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS绿盟科技

本 | 期 | 看 | 点

安全月报

2021年第3期

绿盟科技金融事业部

目录 CONTENTS

安全观点

行业研究

漏洞聚焦

安全态势

安全月报在线阅读

绿盟科技官方微信

NSFOCUS

安全观点

一、事件概述

2021年1月至今，绿盟科技应急响应团队监测到全国多个省份出现多起仿冒银行系统的短信钓鱼事件，其中钓鱼剧本、攻击手法及钓鱼网站页面均高度相似，可基本确认是同一黑产团伙所为。钓鱼短信称受害者手机银行即将过期或账户被冻结，并附带仿冒的钓鱼网站域名。钓鱼网站与目标手机银行登录界面高度相似，并诱导用户输入身份证号、手机号、手机银行登录密码、短信验证码、交易密码等敏感信息。

目前已有多个受害者账户余额被黑产团伙盗刷，请广大用户提高警惕严加防范。

钓鱼短信截图

二、事件分析

攻击者首先通过境外域名注册商注册了大量6至8位的无规律域名，用于后期频繁更换钓鱼网站域名，同时解析地址也均为攻击者在境外购买的VPS。

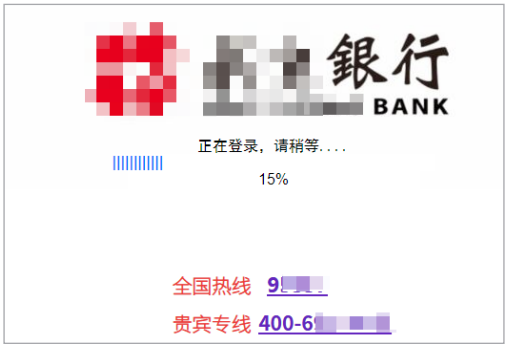
钓鱼域名反查

钓鱼网站首先会判断用户浏览器信息，并诱导用户使用手机浏览器访问。

网站内容伪造为各银行的手机银行登录界面，并要求目标用户输入登录名及密码。

钓鱼网站登录页面

用户输入登录信息后，首先会弹出伪造的登录进度条信息。



同时网站后台会实时调用目标银行身份验证接口，对用户输入的登录信息进行校验，并根据校验结果返回不同的下一步钓鱼页面。

若用户输入的登录信息校验不通过，将返回仿冒的错误信息代码页面。

若用户输入的登录信息校验通过，则返回要求输入交易密码及手机验证码的页面。

在用户提交交易密码及银行发送的手机验证码后，页面将弹出仿冒的账户激活进度条，攻击者此时已在后台通过手机银行进行了转账操作。

在转账前，攻击者还通过某接口获取了受害用户的照片信息，并结合AI换脸技术，绕过了人脸识别校验，并利用银行某些转账功能身份校验缺陷，最终完成转账盗刷。

三、攻击者画像

特征一：专业团伙

该团伙前期做了大量踩点和测试工作，对目标银行的业务系统、业务逻辑及安全漏洞均有所掌握，此外攻击者还对钓鱼网站及VPS做了相应的安全加固措施。

特征二：目标明确

该团伙主要瞄准地方性银行，并根据手机号码归属地向目标银行所在地区的用户发送钓鱼短信。

特征三：精准高效

区别于传统钓鱼网站，此次钓鱼网站会调用目标银行接口校验用户输入的信息，以过滤掉无关错误信息，并实时对上当受害的用户执行转账操作。

特征四：快速转移

该团伙在成功盗取目标银行部分用户的资金后，往往会快速切换域名或更换VPS地址，同时将目标转移至下一个银行，以防止被进一步分析跟踪。

四、安全建议

1. 排查手机银行、微信银行、PC网银等电子渠道系统相关身份认证流程，对存在验证缺陷或漏洞的功能及时进行加固整改。

2. 通过风控系统对高频登录、异地登录、设备切换、单设备多账号登录等异常业务行为进行审计、告警、阻断。

3. 及时更新人脸识别组件版本，提高人脸识别率，或在人脸识别基础上增加双因子或多因子验证措施。

4. 通过手机短信、微信公众号、手机APP等方式，向用户宣传钓鱼诈骗相关防范措施，提高用户网络安全意识。

五、附录

攻击团伙部分VPS地址：

41.216.177.89

203.78.140.153

41.216.177.30

41.216.177.52

156.253.11.4

156.226.23.29

NSFOCUS

行业研究

以蓝军视角跟踪和分析CANVAS 攻击框架泄露事件

——本文分析了 CANVAS 的攻击框架、涉及的漏洞和技术细节

高东

3月3日，绿盟科技研究团队在对网络安全事件舆情监控中发现著名的商业渗透框架CANVAS系统源代码发生泄露，绿盟科技M01N蓝军研究团队第一时间对该事件进行了跟踪，快速分析了CANVAS的攻击框架、所涉及的漏洞和技术细节。

Immunity CANVAS是一套受信任的商业安全评估攻击框架，每月都会发布稳定版本，它允许专业人员进行渗透测试和对手模拟攻击。此次CANVAS的泄露版本为7.26，日期为2020年9月，包含1000+个漏洞利用代码，使用CANVAS成功攻陷系统后，可以抓取屏幕截图，转储密码凭据，操纵目标文件系统并提升特权。攻击者可以在目标系统和目标整个网络区域之间隐蔽连接。另外值得注意的是其中包含Spectre CPU漏洞的可用EXP漏洞利用模块。CANVAS由Immunity开发，该公司由前NSA黑客Dave Aitel创立，然后于2019年出售给CyxteraTechnologies，Aitel于2020年底离开了该公司。

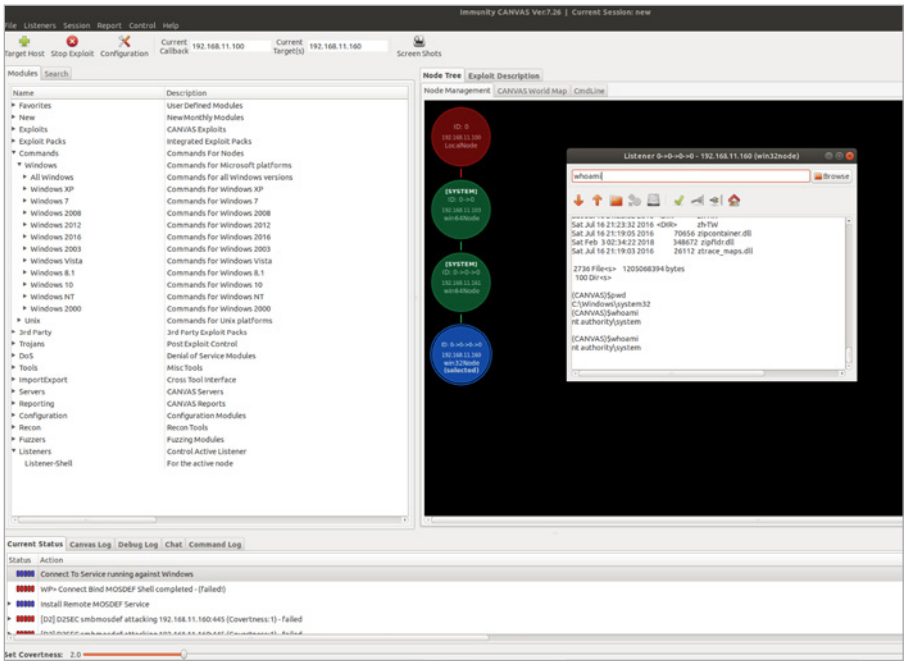
1. CANVAS的框架及主体功能

CANVAS框架主体及模块均使用python开发，支持跨平台安装使用，包括Windows, Linux和MacOSX等, 提供了GUI和命令行来进行操作使用。框架所有功能模块如下：

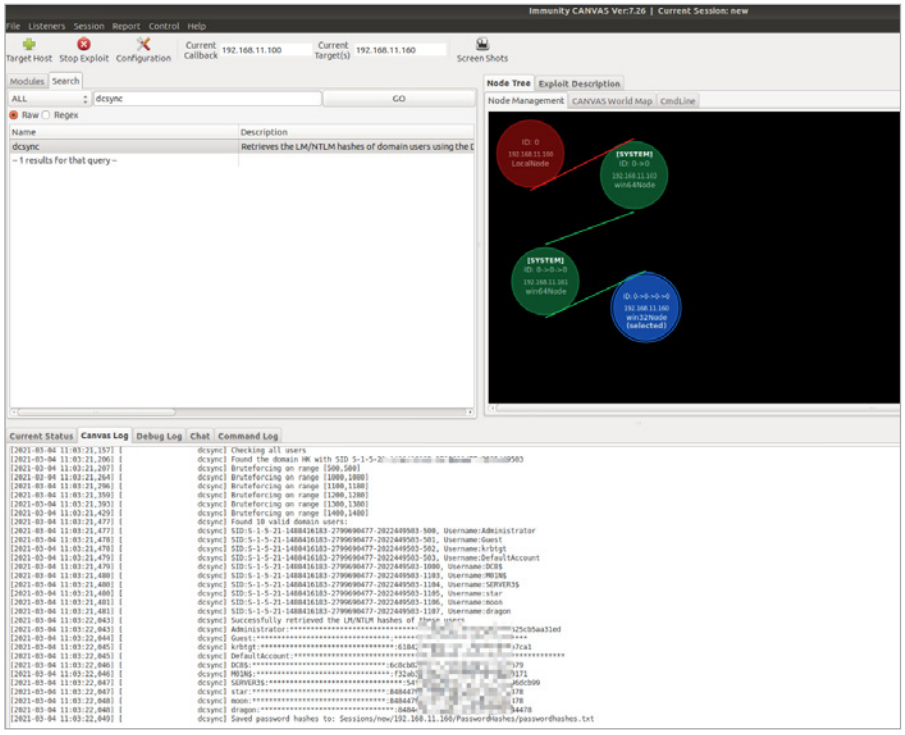
Favorites	使用者自定义归属的常用模块分类
New	最近一次更新中新增的攻击插件或漏洞利用插件：smbghost, smbghost_lpe, men_confusion_lpe, ssrs_viewstate_rec，owa_rce 等
Exploits	CANVAS 自带的各系统平台及应用的漏洞模块
Exploits Packs	第三方的漏洞 EXP 合集
Commands	包含框架进行 C&C 及后渗透所使用的全部控制命令，eg：windows 平台下的 DuplicateToken, GetDrivers 等
3rd Party	第三方漏洞包，自带了 D2ExploitPack
Trojans	完成各场景 Post-Exploitation 所需的核心木马模块，主要为框架核心的 MOSDEF 模块，具备加密和 BypassAV 功能
DoS	包含 DoS 攻击测试所需的漏洞利用及攻击模块
Tools	攻击过程当中所需的其他可用小工具
ImportExport	支持 AVDS、NMAP、NESSUS 等第三方测试软件的报告导入
Servers	完成各类载荷投递及客户端攻击所需的服务模块及代理隧道服务模块
Reporting	评估报告导出功能模块
Configuration	框架配置功能模块
Recon	侦察扫描模块，比如 PortScan, Shareenum, httpfingerprint, userenum 等
Fuzzers	基于 SPIKE Fuzzer 对 TFTP、MSRPC 进行简单 Fuzz 的利用模块
Listeners	打开当前 Node 可用的 Shell 控制窗口

CANVAS主要以漏洞利用为主，功能完整支持攻击链生命周期，包括C&C、权限提升、权限维持、凭证获取、横向移动、防御规避、信息收集、隐蔽隧道及部分域林攻击功能。框架设计以资产节点方式进行攻击过程控制和记录，各节点的远程及本地攻击操作具备完善的攻击日志记录。

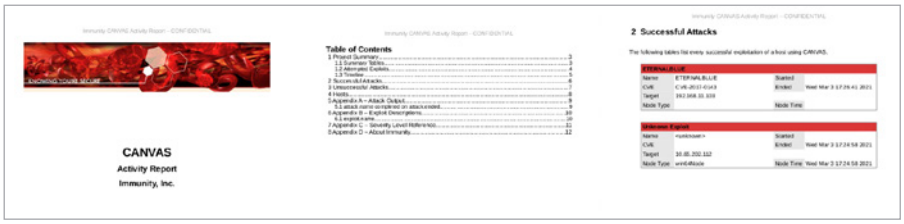
远程漏洞利用、横向移动及C&C功能复现：



成功执行DCSync在测试环境获取AD靶机用户的密码Hash。



同时CANVAS作为一款成熟的商业安全评估攻击框架，具有自动化生成安全评估报告的功能，并且报告拥有良好的可阅读性。

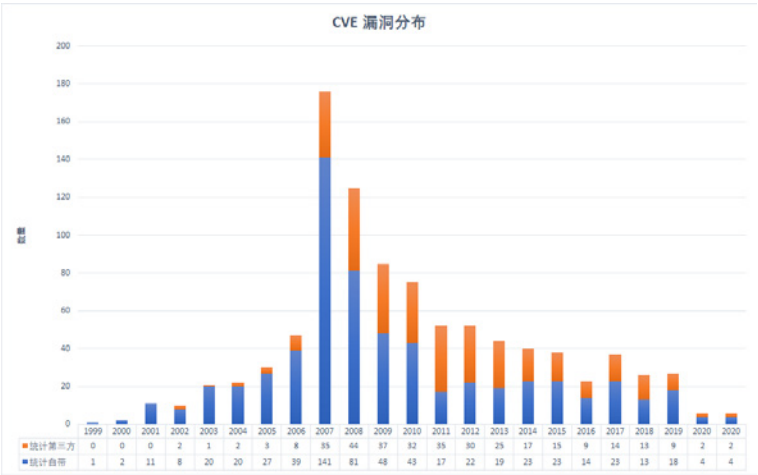


2. 漏洞利用模块

2.1 漏洞利用模块分析

本次泄漏的CANVAS框架源码为次新版本，除自带漏洞利用模块外还包含两大第三方漏洞利用模块，经统计含有CVE编号的漏洞共计929个，框架自带漏洞利用库中包括617个漏洞，第三方漏洞利用库包含333个漏洞，官网上针对工控设备的漏洞利用包Gleg 在本次泄漏中未涉及。

漏洞利用模块	说明
CANVAS	CANVAS 框架自带的 Exploit 模块
D2ExploitPack	来自 DSquare Security 漏洞利用库的第三方漏洞利用模块
White_Phosphorus	来自子公司 White Phosphorus 的漏洞利用库模块



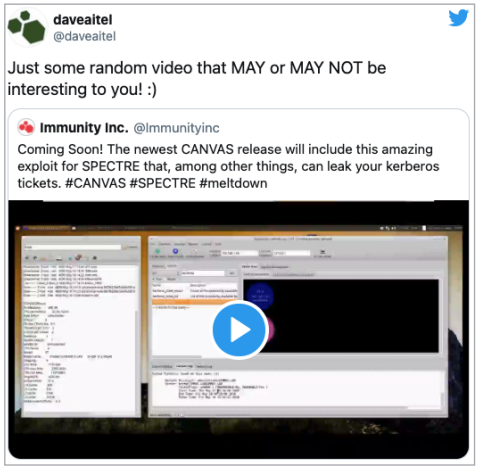
这些漏洞模块在CANVAS中以利用目的大致分为四类，分别针对不同的攻击场景与目标。

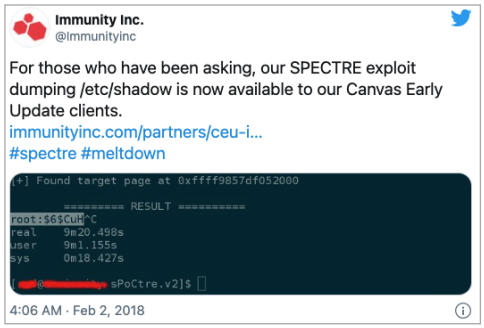
漏洞模块场景分类	说明
Web Exploits	WEB 网站框架或组件漏洞攻击模块，涉及 wordpress,joomla 等漏洞
Remote	针对 Windows 与 Linux 等操作系统以及 cisco 设备的远程漏洞利用模块
Local	针对针对 Windows 与 Linux 等操作系统的本地漏洞利用模块，主要包含本地提权漏洞
Clientside	客户端可利用的漏洞集合，例如 flash 漏洞、ie 漏洞与 acrobat 漏洞，适用于“水坑攻击”场景

2.2 第一个针对Spectre CPU漏洞的可利用EXP

首先我们回顾一下CVE-2017-5715 Spectre CPU漏洞，该漏洞是Intel，AMD和ARM处理器体系结构中的硬件设计缺陷，它允许运行在同一系统上的不良应用程序中的代码破坏不同应用程序的CPU级别之间的隔离，然后从其他应用程序中窃取敏感数据。它的发现以及Meltdown漏洞，被认为是现代CPU演进和历史上的里程碑时刻，有效地迫使CPU供应商重新考虑他们设计处理器的方法，从而明确表明他们不能只专注于性能，而损害了数据安全性。Spectre漏洞从17年被公开开始，研究人员对外公开的均为无害的POC代码，也一直没有发现有被在野攻击利用的证据。

上个月国外安全研究员Voisin发现VirusTotal上的一份Linux Spectre漏洞EXP代码，可以转储/etc/shadow的内容，而近日Dave Aitel的一条推文中，前Immunity首席执行官似乎证实了Voisin的发现确实是他的前公司在2018年2月大力宣传的CANVAS Spectre模块。





当然我们也确认了本次泄露的CANVAS版本确实含有Spectre漏洞EXP插件及代码，代码备注该EXP代码实现在2018年3月完成。

```
#!/usr/bin/env python
##ImmunityHoador v1
################################################################################
## File       :  spectre_file_leak.py
## Description:
##            :
## Created_On :  Thu Mar 22 2018
## Created_By :  X.
##
## (c) Copyright 2015, Immunity, Inc. all rights reserved.
################################################################################

import os
import sys
import struct
import getopt
import datetime
import time
import random
import logging

if "." not in sys.path:
    sys.path.append(".")

from localNode import localNode
from engine.config import canvas_root_directory
from ExploitTypes.LinuxLocalExploit import LinuxLocalExploit
from canvaserror import NodeCommandError
from exploitutils import *

# Specific to kerberos
from libs.kerberos.ccache import CCache

NAME                    = "Spectre File Leak"
DESCRIPTION             = "Dumps /etc/shadow (or any other file) from kernel memory using a Spectre primitive"

DOCUMENTATION           = {}
DOCUMENTATION["CVE Name"]   = "CVE-2017-5753"
DOCUMENTATION["CVE Url"]    = "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753"
DOCUMENTATION["Notes"]      = """
This module gives an unprivileged user the ability to dump a file from the kernel
memory. A common scenario is to dump the /etc/shadow or kerberos tickets.

Note: For Fedora, the attack is targetless while for Ubuntu / CentOS and others
you will need specific offsets compiled within the binary itself.

Caveats:
    1. Attacking vmware is slower, virtualbox while doable is insanely slower.
    2. Sometimes on vmware the KASLR bypass may fail, this is work in progress.
    3. The more recent the processor, the faster the attack.
    4. Not all the filesystems are handled. In particular tmpfs files cannot be leaked.
    5. The attack may not work at all on some specific kernels
    6. The attack may not work at all on some hardware.
    7. With this version you can only dump files fitting within a single page (<= 4096 bytes)

About (possible) future versions:
---------------------------------

a) A cache may be implemented to speedup attempts
b) A completely targetless version (not exclusive to Fedora) may be written later.

"""
```

3. 其他重要功能模块

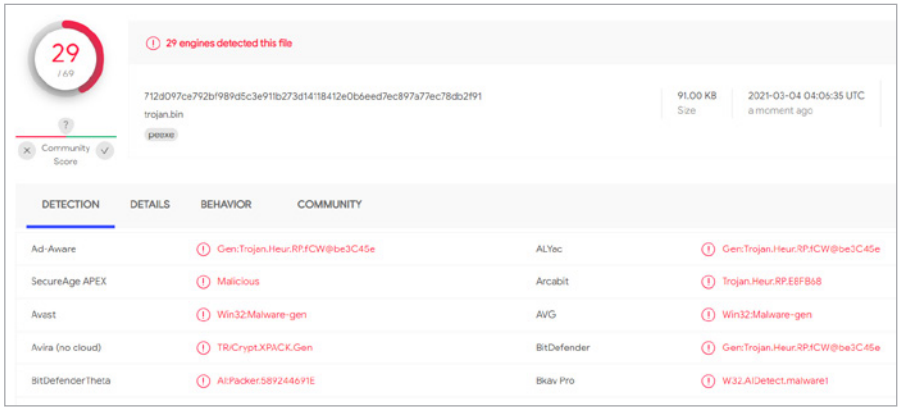
3.1 MOSDEF后门木马

MOSDEF后门木马是CANVAS在命令控制环节的主要模块，其支持主流操作系统，对于一些较冷门的处理器架构亦有较完善的支持。

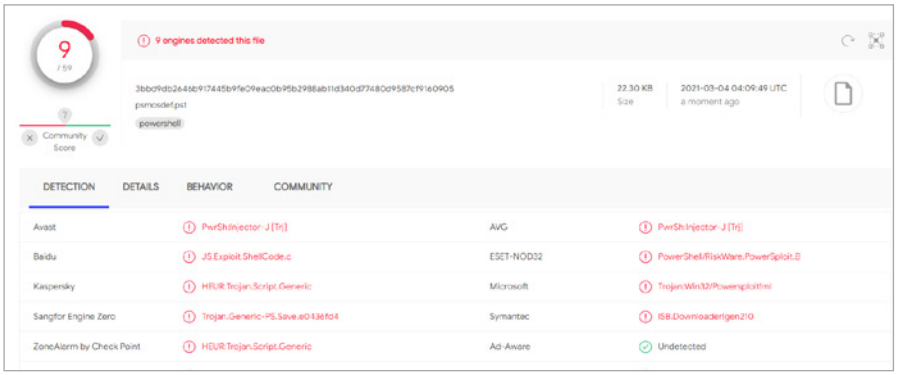
目标操作系统	Windows、Linux、Solaris、Mac OS X
支持架构	x86、x64、PPC、Sparc、ARM
通讯协议	TCP、HTTP、HTTPS、DNS
持久化技术	MOSDEF 服务后门、WMI 事件触发

以防御规避技术研究与攻击检测的视角来看，MOSDEF具有基本的杀软规避功能，支持采用DNS等比较隐蔽的通信方式，具有一定防御规避的能力。其采用的持久化技术等较为常见，所生成的payload类型并不多，但其生成的一些载荷文件在VirusTotal等平台仍具有较好的免杀效果。

根据VirusTotal检测结果，默认生成的Windows x86 版本MOSDEF可执行文件载荷的检出率相对可观。



Powershell版MOSDEF木马具有命令执行、文件上传、执行shellocode等攻击功能，在VisualTotal中具有较低的检出率。



3.2 RootKit模块

CANVAS自带windows与linux系统的rootkit模块，其中windows系统仅有物理内存dump的功能，而linux系统中的rootkit功能要丰富的多。linux平台的rootkit模块以源码的形式分发，每次使用需要针对目标的内核版本进行重新编译内核模块，支持以下功能：

1. 指定名称的文件隐藏

2. 后门进程及子进程PID隐藏

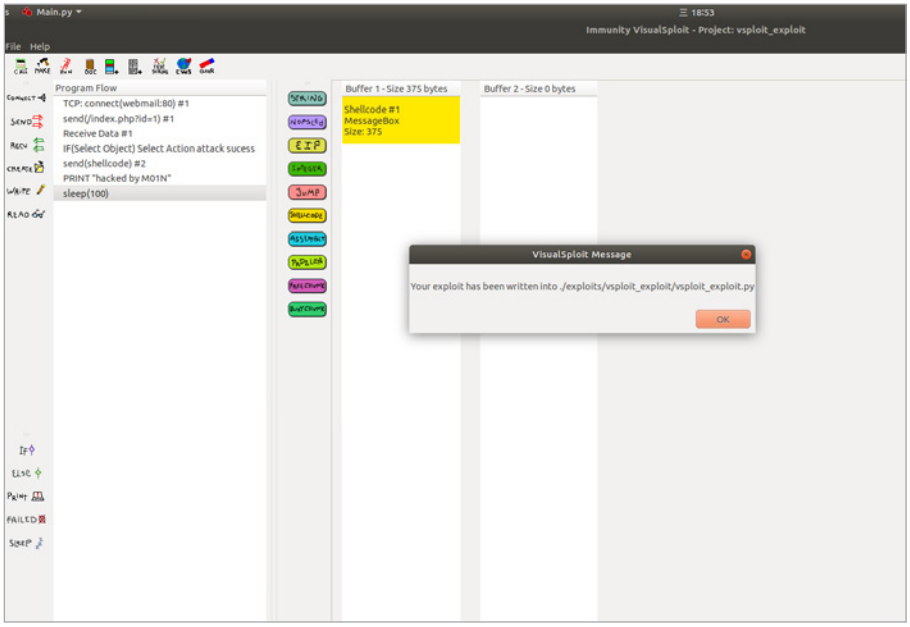
3. TCP通讯隐藏

4. MOSDEF连接后门

利用CANVAS自带的rootkit模块，攻击者可以实现持久化与攻击行为隐藏，增加防守与溯源难度。

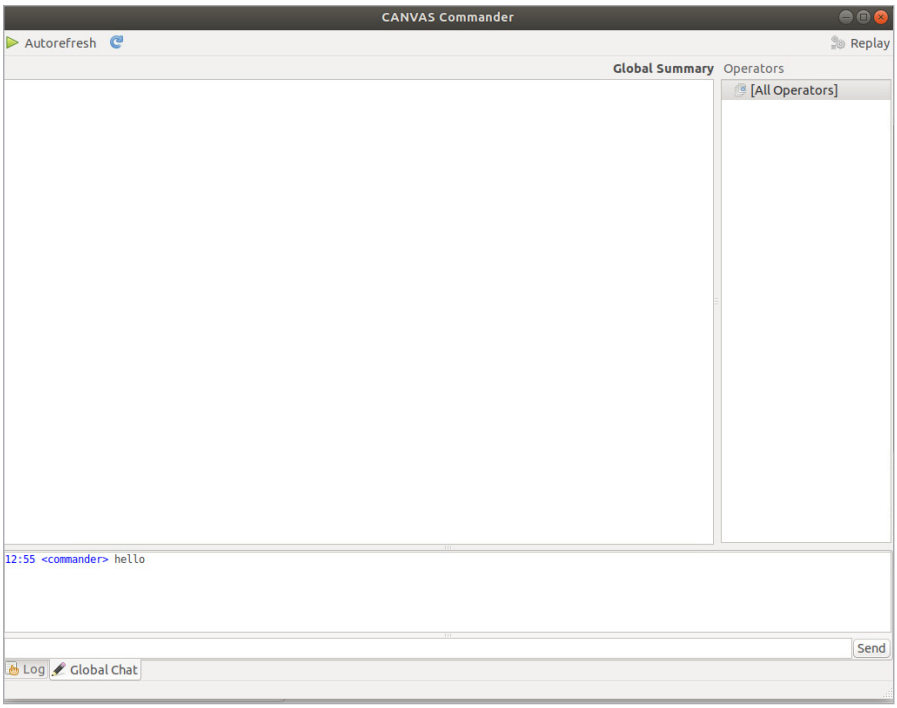
3.3 VisualSploit可视化代码生成工具

泄漏CANVAS包含名为VisualSploit的可视化编程工具，该工具可以进行图形化的exploit开发，设计程序执行流程，操作payload内存布局，最终一键生成可执行python脚本文件。



3.4 协同攻击功能

Canvas Strategic允许在Canvas的多个实例之间进行实时通信，并与中央实例共享信息（目标信息，攻击操作，获得的权限），该中央指挥实例是从Canvas运行Commander模块的机器。当多人作战时，需要对进度和成果进行协协作时，此功能特别有用。此外，它还可以用作多个实例的中央活动监视和日志记录，也包含一个简单聊天服务器。



4. 警惕CANVAS被暴露及滥用带来的风险

本次CANVAS框架源码泄露事件是继NSA泄露DanderSpritz框架后的又一个完整网络攻击框架泄露事件，其中所涉及的TTPs技术已被高度武器化。截止本文公开时我们还暂未实现对CANVAS中的漏洞EXP、持久化技术、隧道技术等技术的全面深入的分析。同时可以看到，本次泄露的漏洞EXP包含全网第一个被公开的针对Spectre CPU漏洞的可利用EXP，另外Powershell版MOSDEF木马在VisualTotal中也同样具有较低的检出率，这些工具都可以直接被恶意攻击者滥用，从而导致严重的安全事故，建议各安全厂商协助企业客户积极防御，防患于未然。绿盟科技M01N蓝军团队将继续跟踪深入分析该框架的内容。

参考链接

https://www.immunityinc.com/products/canvas/index.html
https://spectreattack.com/

Webshell 知多少
——Webshell 威胁分析

一、威胁描述

1.1 Webshell

1.1.1 Webshell 简介

webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。

常见分类：

A. 一句话马
   a. 可认为基于C/S架构（菜刀、C刀、蚁剑、weevely等均有客户端）
   b. 代码简短，体积小
   c. 变形混淆很多

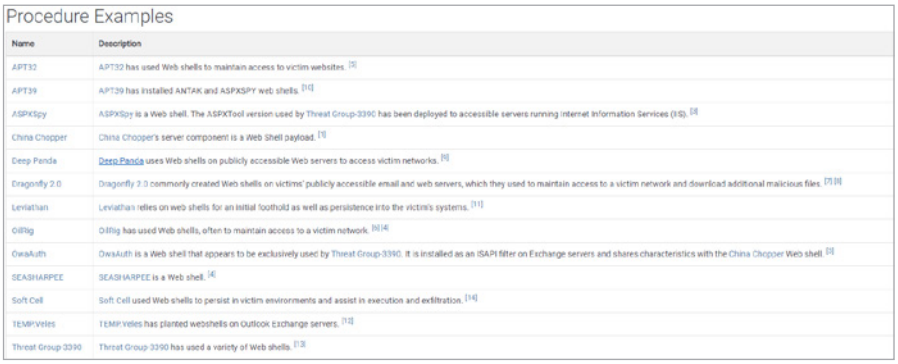
B. 小马
   a. 体积小
   b. 通常仅文件上传功能，用于传大马

C. 大马
   a. 体积大，功能复杂
   b. 调用系统函数如：exec、system
   c. 代码混淆

1.1.2 ATT&CK 相关

所属技术：Persistence（权限维持）

常用组织或示例（https://attack.mitre.org/techniques/T1100/）



Procedure Examples

Name	Description
APT32	APT32 has used Web shells to maintain access to victim websites. [5]
APT39	APT39 has installed ANTAK and ASPXSPY web shells. [11]
ASPXSpy	ASPXSpy is a Web shell. The ASPXTool version used by Threat Group-3390 has been deployed to accessible servers running Internet Information Services (IIS). [3]
China Chopper	China Chopper's server component is a Web Shell payload. [1]
Deep Panda	Deep Panda uses Web shells on publicly accessible Web servers to access victim networks. [6]
Dragonfly 2.0	Dragonfly 2.0 commonly created Web shells on victims' publicly accessible email and web servers, which they used to maintain access to a victim network and download additional malicious files. [7][8]
Leviathan	Leviathan relies on web shells for an initial foothold as well as persistence into the victim's systems. [11]
OilRig	OilRig has used Web shells, often to maintain access to a victim network. [9][4]
OwaAuth	OwaAuth is a Web shell that appears to be exclusively used by Threat Group-3390. It is installed as an ISAPI filter on Exchange servers and shares characteristics with the China Chopper Web shell. [3]
SEASHARPEE	SEASHARPEE is a Web shell. [4]
Soft Cell	Soft Cell used Web shells to persist in victim environments and assist in execution and exfiltration. [14]
TEMP.Veles	TEMP.Veles has planted webshells on Outlook Exchange servers. [12]
Threat Group-3390	Threat Group-3390 has used a variety of Web shells. [13]

图1.1 植入、利用过程

APT 特征：

表1.1 APT攻击信息

组织	攻击对象	针对组件	攻击入侵方式	补充
Emissary Panda (AKA APT27，TG-3390，Bronze Union, Lucky Mouse)	Government Organizations of two different countries in the Middle East。（中东 2 个国家的政府组织）	SharePoint	CVE-2019-0604	后续利用工具探测 CVE-2017-0144
特征	1. 利用 webshell 上传合法 exe 加载恶意 DLL,HyperBro	INISafeWeb SSO.exe	inicore_v2.3.30.dll	https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
	2. webshell 路径：/_layouts/15/error2.aspx /_layouts/15/errr.aspx	Antak webshell	参数 MD5(t)	

1.1.3 植入 & 利用

图1.2 植入、利用过程

二、检测方法

2.1 流量检测

2.1.1 场景描述

当前流量检测设备UTS（包含WAF规则、IDS规则、基于文件及基于流量的机器学习检测）/IDS/IPS的检测规则均可分为2种检测方式：

1. 基于流量还原脚本文件，检测文件中的特征判定webshell。该类检测通常表现为产生XX webshell 上传/下载告警。

2. 基于连接webshell进行恶意活动的流量检测。该类检测通常表现为产生XX webshell访问控制告警。

2.1.2 IPS / 全流量检测及分析

1. 仅基于IPS的检测分析可参考通用webshell的研判检测，主要思路为：
   a. 确认给出的告警属于webshell访问控制的告警
   b. 判断webshell是存在（响应码200 ok）。为精确自动化判断目前需要，排除响应404页面但200 OK 响应码的情况（3XX跳转情况）。步骤可参考如下，
      a) 探测工具自动请求时，任意构造一个路径如,XXXXX/XXXXXX.jsp保存响应码XX_code响应内容XX_content。
      b) 提取访问通信的webshell目标webshell_URL，访问获取响应码webshell_code,响应内容webshell_content。
      c) 若webshell_code = XX_code则基本断定为404页面响应但给出200 响应码场景（或是3XX跳转，则跟进）。若XX_content 和webshell_content对比类似则可基本判断该webshell文件不存在服务器上。
      但若XX_content 和webshell_content对比具有较大差异，可能为2个路径不同错误响应页面或者404页面伪装webshell。此时给出上述code、content人工判断。
      d) 若webshell_code ！ = XX_code则可能webshell文件存在，给出告警，人工核实。
   c. 判断webshell是否能被服务器解析，ips系建议人工判定
2. 全流量系的流量研判
   a. 确认给出的告警属于webshell访问控制的告警
   b. 判断webshell真实存在服务器端（参考IPS判断方式，但建议从主动访问提取http访问记录。如提取404响应的http_log中的响应内容等字段）
   c. 判断服务器能否解析webshell
      i. 上述2个步骤基本可判断是否存在webshell，还可基于响应内容进行进一步精确匹配。以下给出2016版菜刀及蚁剑的响应示例。

```
(root:/) $ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

图2.1 蚁剑客户端执行”ls”

```
TTP/1.1 200 OK
Date: Wed, 23 Oct 2019 14:07:22 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 117
Connection: close
Content-Type: text/html; charset=UTF-8
```

图2.2 Webshell响应”ls”头部

```
cc89fe9faa3fbin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
[S]
/
[E]
d91fa085fb
```

图2.3 Webshell响应”ls”body

发现上述除响应码特征外，蚁剑的命令执行响应特征包含：起始及结束均为一串16进制数（上述响应体的起始16进制数和命令执行的结果粘连），其中包含命令执行的结果。而结尾处以[S]和[E]作为命令执行的当前目录。而其命令执行的内容在请求头中可进行分析。如下图所示：

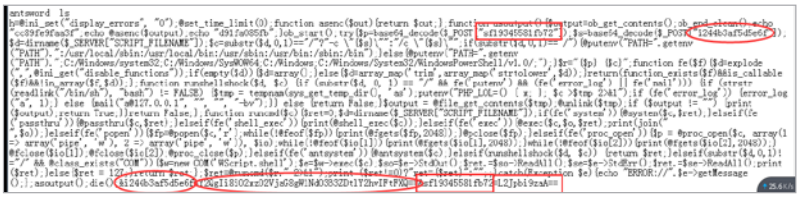


图2.4 Webshell请求头的post体

cd "/";ls;echo [S];pwd;echo [E]	Y2Qgli8iO2xzO2VjaG8gW1NdO3B3ZDtlY2hvIFtFXQ==

图2.5 Webshell请求头关键命令

/bin/sh	L2Jpbi9zaA==

图2.6 Webshell请求头关键参数

菜刀的交互和蚁剑交互类似，仅是以“X@Y”作为响应内容的分割，下面给出菜刀交互的示例：

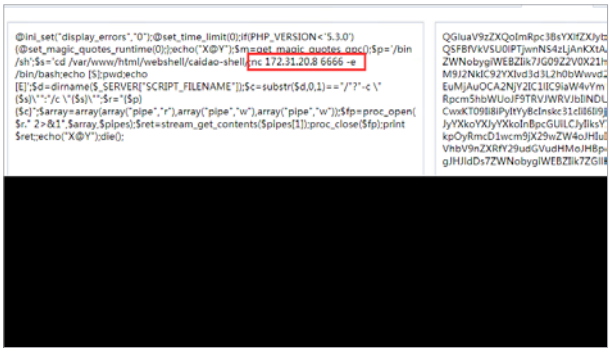


图2.7 菜刀交互示例

图2.8 菜刀请求执行参数

ii. 方法i中的方法可直接判定webshell的存在且获取到执行的命令及结果。若无法从请求及响应中直接研判能否进行解析等，可通过下述方式进行webshell有效性的计算：

a) 获取http_log中响应码200 对应请求体提取URL，提取文件后缀名如php、jsp等，通常可表明能够进行该类文件解析。

b) 丰富资产管理模块，记录脚本语言、web框架等内容。再调用该模块的记录（主要为开发语言）判断是否能够解析（还可以用于初步研判其他入侵攻击是否生效）。方法参考whatcms，总的来说为提取特定js、响应体特征匹配。参考链接，https://github.com/HA71/WhatCMS

iii. 统计学方法给出webshell可疑度计算。

在i和ii中已经对已知、有特征的webshell进行了检测告警，但存在未在知识库的webshell（如通信加密、定制化webshell等）。针对该些webshell可通过一定统计特征进行威胁程度的评分对评分大于一定阈值的文件进行告警。

1. 提取新增的url为x-url（post请求且响应码200，去除开发不规范参考ii方法。）
2. url中含update、webshell、shell等已知类似shell文件的命令或是名字信息熵较大。威胁评分增加，匹配上已知webshell占总评分权重60%。信息熵越大勤奋越高，整体不超过权重20%。
3. 在一定时间内持续获取x-url入度（http_log中url为x-url的不同referer的个数）、出度（referer为x-url的不同url个数）。出入度越少，威胁程度越高（整体权重设置小于10%）
4. 获取源IP，源IP较少时（可定量且可调整如3、或是根据总访问量进行计算），分析一定周期内源IP行为。根据源IP行为给改页面进行威胁性评分（alert_log中处在攻击记录、目录扫描【http_log请求频率高且异常响应多】，权重占比不超过20%）
5. 计算请求/响应（一定周期访问量top x）的信息熵、重合指数、最长单词作为范围基线或是平均后做基线。计算x-url请求/响应的信息熵、重合指数、最长单词和基线作比较，信息熵越高、重合指数越低、最长单词越长（权重最低）。（整体权重占比不超过60%）
6. 当上述评分相加超过阈值如60时进行告警，或是某个区间时进行终端检测的介入。

2.2 终端检测及响应

2.2.1 文本静态检测及响应——需要测试下文件隔离

1. EDR检测及响应

(1) 场景

① 基于流量的检测存疑需要介入终端文件检测（手动|事件触发）

② 加密通信，流量无法进行检测或是需要确认的场景（事件触发|闲时定时任务）

(2) 检测原理

目前主流的基于文件的webshell查杀包含了正则匹配、webshell沙盒、深度学习模型。

当前EDR的检测主要为静态检测，对脚本文件中所使用的关键词、高危函数进行检测。该种方式的特点是基于已知的webshell提取的特征，对于一些未知（如黑名单外的回调函数或是请求头等特定构造的webshell等）或者一些混淆的webshell难以被检测。

但基于文件的webshel检测可补足基于流量时被加密而服务器端的webshell文件存在特征的情况。同时主机端可收集文件修改的时间、文件权限、文件的所有者以及和其它文件的关联性等多个维度的特征进行检测。

(3) 告警情况

从使用的一些变形、混淆的脚本来看，绕过静态文本检测的成本太低。但该检测方式仍是在终端环境下检测已知webshell的基础方法。目前测试1500多个样本，EDR检测告警1049个，D盾告警1197个。以下给出检测结果示例：

图2.9 菜刀请求执行参数

(4) 事件真实性确认

当基于文件检测告警出webshell时，可通过以下维度进行判断：

a. 告警的威胁程度进行快速判断（EDR中为高危、D盾威胁等级3及以上）。

b. 关联流量日志，获取初次访问的IP，追溯历史行为。若存在高危攻击、目录遍历等行为则更具对应行为进行威胁度评分。

c. 通过获取文件属性如创建时间、修改时间、文件权限、所有者等进行可疑度评价。

d. 人工获取文件内容进行识别，分析。从函数作用，代码可读性等进行分析。人工识别时可借助其他工具进行配合判断。可使用如下检查工具：

表2.1 TAM事件

编号	名称	参考链接
1	网站安全狗网马查杀	http://download.safedog.cn/download/software/safedogwzApache.exe
2	D 盾 Web 查杀	http://www.d99net.net/down/WebShellKill_V2.0.9.zip
3	深信服 WebShellKillerTool	http://edr.sangfor.com.cn/tool/WebShellKillerTool.zip
4	BugScaner killwebshell	http://tools.bugscaner.com/killwebshell/
5	河马专业版查杀 Webshell	http://n.shellpub.com/
6	OpenRASPWEBDIR+ 检测引擎	https://scanner.baidu.com
7	深度学习模型检测 PHP Webshell	http://webshell.cdxy.me/

(5) 基于EDR的响应

目前EDR可针对存在问题的文件进行隔离，则针对上诉检测结果可尝试实现：

a. 自动隔离(流量检测或是文件检测完全确认时，用于需要快速响应的关键时期)

b. 根据告警手动隔离

c. 主机隔离

EDR文件隔离实现原理：

根据测试，当前EDR实现文件隔离的原理是重命名修改的文件，将其后缀修改为q00，这种方式在web服务中访问原文件会报404（文件重命名，原文件不存在），但访问原文件名+q00后缀可以文本的形式读取该文件。

2.2.2 Linux 终端日志检测

1. 场景

   关键点：

   a. webshell命令执行会调用syscall

   b. syscall的调用可审核

   描述：

   webshell可视为web应用的一个脚本，其执行命令时均通过调用web开发语言中已经实现的模块进行，如python中的OS模块中的system()函数、php中的exec()函数、java中的Runtime.getRuntime().exec()等等。调用该些函数在系统不会像用户在shell中执行命令一样结果记录到history中，但通过针对web服务执行用户的syscall调用审核可发现命令执行活动。同时结合web服务通常的行为特征，可判断该命令调用是否为正常情况。结合流量日志、web访问日志等可定位到发起该调用行为的原因。

2. 检测方法

   a. 依赖服务：

      audit(OS query中可通过配置audit实现部分检测)

   b. 检测原理：

      监控web服务所在用户的syscall调用，实现对异常系统调用的检测。示例：通常攻击者拿到webshell时，会执行命令查看权限如：whoami，查看网络环境如：ifconfig或是读取非web服务目录相关文件如：/etc/passwd等等。该些调用均可通过audit制定相应的审计规则来审计，监控web服务所在用的异常syscall调用及文件操作。故可优先针对敏感操作进行直接告警，再对web服务的调用操作建立基线包含通常调用的syscall及文件操作等。再对偏离基线的操作进行告警或是关联日志其他日志进行再次计算。

   c. 日志分析

      从/var/log/audit/audit.log中可查看自定义规则(审计uid=web服务所在用户的syscall)产生的日志。如图2.11：

图2.10 菜刀命令执行日志-audit

图2.11关键信息解释：

日志类型：SYSCALL，记录信息-msg：audit(timestamp：slog_id),父进程id：ppid, 用户id：uid,执行命令：sh,可执行程序：exe,自定义规则名称：key,执行进程id:pid。

则图2.11的SYSCALL日志获取到信息，时间为1572257580，uid为48的用户通过父进程ppid=1726调用exe=/usr/bin/bash.mjs.1，执行命令comm=”sh”，触发规则为key=webshell_command。

日志类型：EXECVE，通过log_id和SYSCALL日志关联到一条记录。获取执行命令时的参数。如a2，该参数值为16进制数据，将其转换为16进制即可得到执行的命令情况（可参考2.1.4中流量检测对菜刀流量的分析示例），如图2.12：

图2.11 菜刀命令执行日志-EXECVE

日志类型：CWD，通过log_id关联到一条纪录，记录命令执行的所在目录cwd=/var/www/html/webshell/caidao-shell

通过日志记录，即可获取调用SYSCALL执行的命令、时间信息、父进程信息、用户信息、工作路径、触发规则等信息。

3. audit检测特点

该方式实际是审计用户和内核的交互情况，通常可实现：监控文件访问，监控系统调用。而2.2.2的第2小结监控的为apache用户调用的SYSCALL。该监控并非仅能实现对webshell的执行命令的检测，还能对一些命令执行漏洞进行检测

（包括0day，需要区分正常和异常SYSCALL调用。考虑UEBA实现）。

该方式对webshell源码经过混淆、通信流量进行了加密的情况具有检测优势。

2.2.3 Windows 终端进程检测

1. 场景

当webshell通过web应用执行命令时，通常会通过web服务中间件调用cmd、powershell等程序执行命令。故可通过对web应用的进程活动进行检测，发现异常执行的命令，及定位发起该行为的文件。

2. 检测方法

a. 依赖工具（监控进程行为即可）

火绒剑

OSquery中进程监控（但未经测试）

b. 检测原理

核心还是基于异常的检测模式，检测web服务进程是否存在可疑的操作，如通常攻击方取得webshell后会执行cmd、whoami、net user等操作。该部分操作通过web服务的进程（或是子进程）调用对应的可执行文件完成。故可对web服务进程的调用进行检测，发现异常情况。该部分可尝试2种检测模式（或是同时采用）：

内置敏感文件c:\boot.ini、c:\windows\repair\sam及可执行程序cmd、ipconfig、whoami等的访问告警。

对web服务通常访问调用的程序建立基线，偏离基线的进行告警。

c. 日志分析

分析在webshell中执行whoami的文件调用访问过程，可获取到weshell执行的命令情况。

i. 获取执行命令的文件

如下图php-cgi.exe（fast cgi模式下的脚本解析进程）开打文件test2.php后又打开和执行了可执行文件cmd.exe。则目前从时间关系上判断产生调用cmd.exe程序的文件很可能为test2.php。

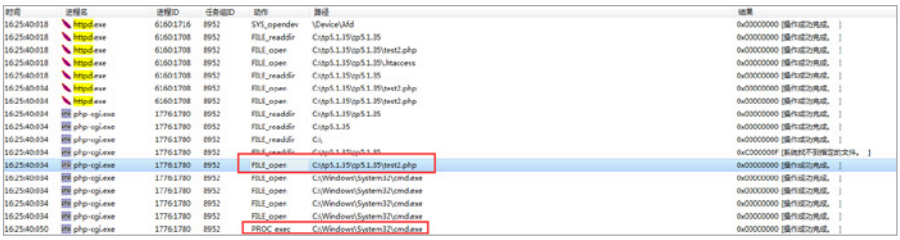


图2.12 服务中间调用情况

ii. 发现php-cgi.exe执行cmd.exe后，查看其执行详情中的动作，可获取到cmd.exe执行的子进程id：10928。

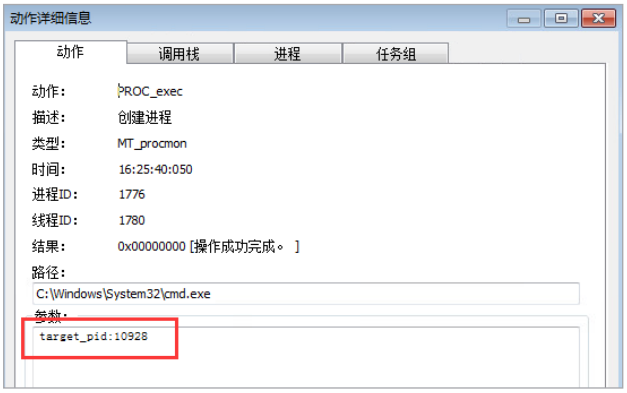


图2.13 服务中间调用情况

iii. 跟进上述子进程的参数，可获取到执行的详细命令情况。如下图2.14。

图2.14 服务中间调用情况

综合上述的分析可获取到信息：php-cgi.exe在解析test2.php时调用了cmd.exe且在cmd.exe中获取到输入的关键参数net user。则通过该过程发现疑似webshell文件。后续进行溯源时可通过流量等信息管理事件进行定位。

三、综合分析

3.1 简述

该部分尝试关联流量检测、静态样本分析、主机审计日志、统计分析、资产比对等方式对可疑的webshell文件进行评价，确认是否需要进行响应处置。

3.2 异常syscall关联分析

3..2.1 关联日志分析

场景：

监控SYSCALL等的调用，发现异常时可提取到父进程，用户等信息。若仅有终端方面的数据，可进行如下分析。

关联分析：

1. 分析还原进程调用情况

① 在audit记录的日志中提取ppid（命令执行父进程）、调用的程序、执行的进程号、执行命令。如在2.2.2中第二小节获取到。uid为48的用户通过父进程ppid=1726调用exe=/usr/bin/bash.mjs.1，执行命令comm=”sh”，执行进程ID=3510。

② 根据ppid获取产生调用的进程及其父进程，如使用PS获取到ppid的进程为httpd，该父进程的上一进程为1441的httpd进程。则表明为web中间件发起的调用。如图3.1：

```
   1  1441  1441  1441 ?           -1 Ss       0   0:02 /usr/sbin/httpd -DFOREGROUND
1441  1610  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
1441  1725  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
1441  1726  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
1441  1727  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
1441  1728  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
1441  1729  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
1441  3431  1441  1441 ?           -1 S       48   0:00  \_ /usr/sbin/httpd -DFOREGROUND
```

图3.1 进程定位-0

③ 还原进程调用情况：

initd

-httpd 1441

-httpd 1726

-/usr/bin/bash.mjs.1 -/bin/bash -c xxxx

④ 定位发起调用的用户：

根据uid读取/etc/passwd即可获取用户名及其权限信息等，如图3.2：

```
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

图3.2 进程定位-1

2. 分析，定位异常的webshell

① 根据SYSCALL判断异常命令执行。及进程情况判断为web应用执行的异常调用。

② 根据log_id关联的CWD获取到路径cwd对应的值，确认疑似webshell的文件目录。获取调用时间戳timestamp。

③ 获取web访问日志，根据时间及路径信息获取提取可疑的文件。过程如下：

获取时间如图3.3

图3.3 进程定位-2

获取文件所在目录如图3.4

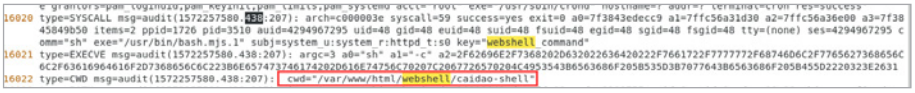


图3.4 进程定位-3

关联web访问日志（也可通过该方式关联，TAM中的http_log），定位webshell可疑文件：p.php。

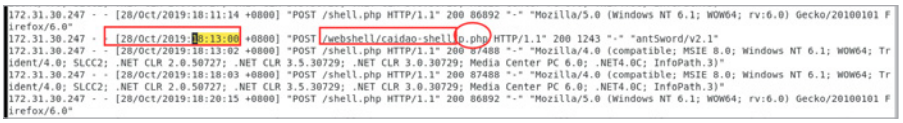
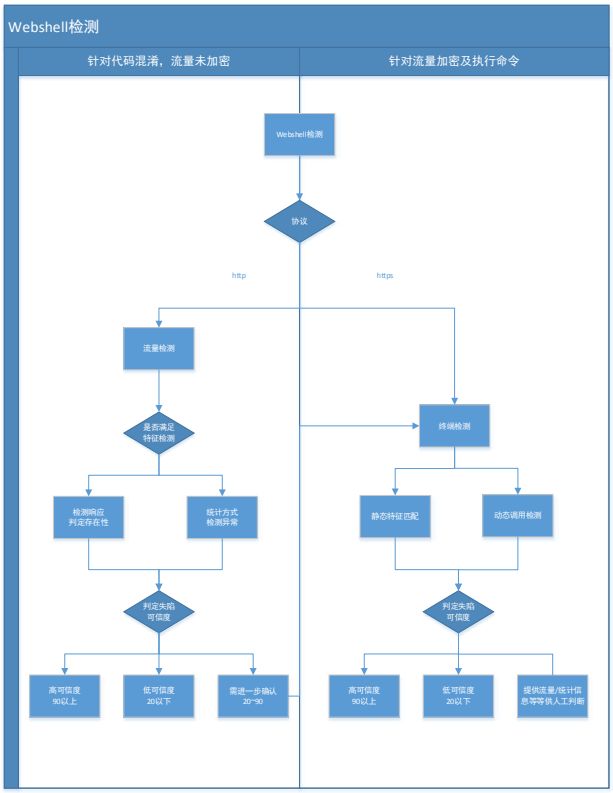


图3.5 进程定位-4

该方式目前强关联的点为时间戳（ms级）和访问路径，在访问量很大的情况下可能会出现一些时间相同且路径一致的情况。若后续出现大量2者一致的情况，可调用静态文件查杀或是文件属性相关信息做综合判断。

四、整体模型

4.1 整体模型



公安部：去年抓获侵犯公民个人信息犯罪嫌疑人 9700 余名

摘　要：公安部新闻发言人贾俊强26 日表示，2020 年全国公安机关共侦办侵犯公民个人信息刑事案件3100 余起，抓获犯罪嫌疑人9700 余名，侦办治安案件3400 余起，处理违法人员3600 余名。

关键词：标签（个人信息），技术问题（安全事件）。

内　容：公安部新闻发言人贾俊强26 日表示，2020 年全国公安机关共侦办侵犯公民个人信息刑事案件3100 余起，抓获犯罪嫌疑人9700 余名，侦办治安案件3400 余起，处理违法人员3600 余名。

在26 日上午公安部举行的新闻发布会上，有记者问：侵犯公民个人信息问题历来备受社会关注，也是近年来两会代表委员关注的热点。请问2020 年公安机关在打击侵犯公民个人信息犯罪方面有哪些举措和成效?

贾俊强回应称，近年来，侵犯公民个人信息违法犯罪活动十分猖獗，不仅严重侵害群众的人身权益，也容易诱发电信网络诈骗、盗刷银行卡等下游犯罪，群众对此反映强烈。

2020 年，全国公安机关以“净网2020”专项行动为契机，聚焦人民群众深恶痛绝的侵犯公民个人信息犯罪，持续开展集中打击行动，不断压缩侵犯公民个人信息违法犯罪活动空间。

贾俊强表示，据统计，2020 年全国公安机关共侦办侵犯公民个人信息刑事案件3100 余起，抓获犯罪嫌疑人9700 余名，侦办治安案件3400 余起，处理违法人员3600余名，有力打击了犯罪分子的嚣张气焰，有力维护了网络空间秩序和人民群众合法权益。

贾俊强指出，特别是2020 年初，因新冠肺炎疫情导致的恐慌情绪在网上蔓延，涉疫情人员个人信息在网上泄露的问题引发社会广泛关注。公安机关迅速行

动，严厉打击侵犯涉疫公民个人信息违法犯罪，共治安处罚违法人员1500 余名，通报有关部门给予党纪政纪处分430 余人，及时震慑了违法违纪人员，有力保护了涉疫情公民合法权益，为抗疫工作营造了良好社会氛围。

贾俊强称，与此同时，公安机关对侵犯未成年人、老年人公民个人信息等犯罪活动重拳出击，破获窃取贩卖未成年人和老年人个人信息案件50 起，打掉团伙43 个，抓获犯罪嫌疑人860 余名；查获重点行业内部涉案人员500 余名，破获案件94 起；破获利用“暗网”等侵犯公民个人信息犯罪案件91 起，抓获犯罪嫌疑人220 余名；破获窃取、贩卖人脸数据案件22 起，抓获犯罪嫌疑人60 名。

贾俊强提示，对于来源不明的链接、网站等，请谨慎填写个人信息，谨慎下载、使用来源不明的手机APP。一旦发现个人信息被泄露、非法获取和使用，及时向公安机关报案。

信息来源：https://mp.weixin.qq.com/s/yAztAhNyHiL3-ePnJyHy3g

被控非法侵犯用户隐私，TikTok 同意支付 9200 万美元进行和解

摘　要： 近期，TikTok 的母公司字节跳动已经同意向美国用户支付高达9200万美元的和解金。这些用户在前段时间对TikTok 进行了集体诉讼。

关键词： 标签（TikTok、用户隐私），技术问题（安全事件）。

内　容： 这些用户在前段时间对TikTok 进行了集体诉讼，他们指控TikTok 在没有得到他们同意的情况下使用“复杂的人工智能（AI）系统”来识别用户视频中的面部特征，并推荐贴纸和滤镜，还引用算法作为识别用户的年龄，性别和种族的手段。该诉讼还指控用户数据未经同意即被发送到中国，并与第三方共享。而这些都违反了伊利诺伊州严格的隐私法。

伊利诺伊州的生物识别隐私法异常严格，该法允许用户起诉那些未经同意收集消费者数据的公司。同时，伊利诺伊州是唯一一个允许人们对这种未经授权的数据收集行为要求金钱赔偿，并且有相关法律支持的地区。隐私倡导者称赞该法律是国家在数据商业化形势中最强有力的保护形式，它在科技巨头和其他企业的不断削弱中幸存下来。

在严格的法律之下，字节跳动并不是第一家被指控的公司。在去年2 月，Facebook也收到了同样的指控，并且最终同意支付5.5 亿元的和解费。

在遭到诉讼之后，TikTok 在1 月宣布将对年轻用户进行更严格的审查，包括进行默认的隐私设置，并将Duet 和Stitch 限制为16 岁及以上的用户。但或许是因为有Facebook 的前车之鉴，同时也避免长时间的诉讼造成对于公司的负面影响，在否认了有任何不当行为之后，字节跳动仍然同意了通过支付和解金来摆脱诉讼。

对此，TikTok 发表了一份声明称："虽然我们不同意这些说法，但与其经历冗长的诉讼，不如集中精力为TikTok 社区打造安全和快乐的体验。"

但在同意支付和解金之后，TikTok 的和解协议还必须得到联邦法官的批准，协议被批准之后，TikTok 才能真的从这场诉讼中脱身。

这次并不是TikTok 第一次被美国陷入危机，自特朗普对其颁布禁令之后，TikTok可谓是步履维艰。之前，美国政府就已多次怀疑TikTok 将美国用户的信息传送至北京，并以此为借口对其作出制裁。并且在去年，美国政府多次发布针对TikTok 的出售令，想要逼迫字节跳动将其美国业务出售给微软以及甲骨文，好在这项出售令如今随着特朗普的下台而无限延期。虽然在新总统上任之后，拜登政府对于TikTok 的态度不似前政府那样咄咄逼人，但这一次的隐私诉讼很难让人不想到地缘政治的因素。

字节跳动的创始人张一鸣在遭遇特朗普威胁的时期曾接受采访表示，TikTok 不会放弃全球化的脚步，高达1 亿用户的美国市场自然是他们全球市场中不可或缺的一部分。如果TikTok 想要继续在美国有良好的发展，就要做好长期面对来自美国政府的控诉的准备，如何与其周旋并发展其业务，是字节跳动全球化发展中最重要的策略。

信息来源：https://www.freebuf.com/news/264839.html

加密货币诈骗盗取 1600 万美元

摘　要： 近日，一名瑞典商人承认，他通过反向养老金加密货币投资骗局骗走了数千名受害者数百万美元。

关键词： 标签（加密货币、投资诈骗），技术问题（安全事件）。

内　容： 该名商人名叫乔纳斯·卡尔森，他受到了证券欺诈、电信欺诈和洗钱的指控，指控称他诈骗了3575 名受害者超过1600 万美元。

2019 年3 月4 日，卡尔森和他现已倒闭的公司东方金属证券在一份刑事起诉书中被起诉。这名47 岁的男子使用至少六个不同的化名，包括欧几里德·德罗里斯和帕拉蒙·拉拉斯软。三个月后，他在泰国被捕，并被引渡到美国。

从2012 年11 月到2019 年6 月，卡尔森和EMS 使用网站www.easternmetalsecurities.com 作出虚假陈述，并说服受害者使用虚拟货币购买“预备资金的反向养老金计划”（PFRPP）中的股票。

受害人被承诺最终以每100 美元的价格支付1.15 公斤黄金。卡尔森向投资者保证，如果不支付黄金，他将退还其投资的97%。

实际上，卡尔森把投资者给他的钱转到了自己的个人银行账户上，然后用这笔钱在泰国购买了昂贵的住宅和一个度假胜地。他向美国当局承认，他没有办法偿还投资者。

此后，卡尔森利用第二个网站www.hci25.com，与潜在的投资者进行了多次虚假交流，目的是推迟投资者意识到自己无法收回资金的那一刻。

根据美国加州北部地区法院发布的逮捕令，www.easternmetalsecurities.com网站现已被查封。

卡尔森因电信欺诈和证券欺诈指控面临最高20 年监禁和最高25 万美元罚款，因洗钱指控面临最高20 年监禁和最高50 万美元罚款。

信息来源：https://mp.weixin.qq.com/s/SzQC9_YSNWuZaV7gYy_ncw

黑客入侵 15 万个 Verkada 监控摄像头

摘　要： 近日，据彭博社报道，黑客入侵并访问了特斯拉、Equinox、多家医疗诊所、监狱以及犹他银行在内多家企业的实时监控摄像头。

关键词： 标签（黑客入侵、Verkada、监控摄像头），技术问题（安全事件）。

内　容： 近日，据彭博社报道，黑客入侵并访问了特斯拉、Equinox、多家医疗诊所、监狱以及犹他银行在内多家企业的实时监控摄像头。

除了从摄像机捕获的图像外，黑客还分享了屏幕截图（下图），证明他们成功通过root shell 访问了Cloudflare 和特斯拉总部的监视系统。

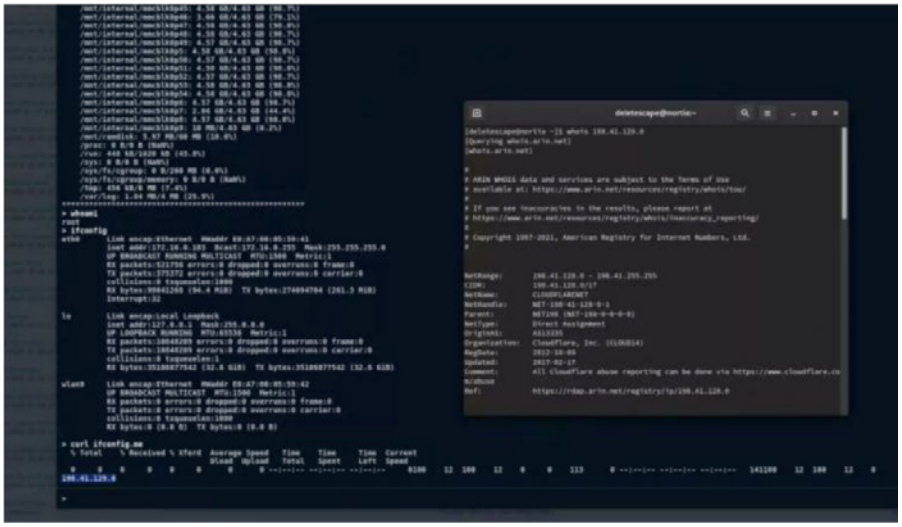
黑客晒出的特斯拉总部仓库的监控视频截图

根据黑客组织的逆向工程师Tillie Kottmann 的说法，他们使用Verkada 的超级管理员帐户访问了这些监视系统，Verkada 是与上述组织合作的监控设备公司。

Kottmann 向Bleepingcomputer 透露，他们在公开的DevOps 基础架构中找到了Verkada 超级管理员帐户的硬编码凭据。

Verkada 生产企业安全系统，例如自动化和IoT 监控摄像头，其知名用户包括特斯拉。

在同一推特会话中，Kottmann 还分享似乎是对Linux 操作系统的根访问权限的截图。从这些截图中，可以看到其中一个网卡的MAC 地址，该地址与监视公司Verkada开发的设备相对应。



黑客证明已经获得了对Cloudflare 和Tesla 系统的Shell 访问权限

据悉，在首次报道该攻击事件的彭博新闻社联系Verkada 之后，黑客失去了被黑客攻击的超级管理员帐户的访问权限。

Verkada 在一份声明中表示：“我们已禁用所有内部管理员账户，以防止任何未经授权的访问。我们的内部安全团队和外部安全公司正在调查此问题的规模和范围，并已通知执法部门。”

此次网络攻击在社交媒体上的主题标签是：#OperationPanopticon，其中Panopticon 是一种监禁建筑的设计概念，使俘虏（例如囚犯）无法确定在给定时刻是否有安全人员监视。

这意味着，在一个有大量囚犯的建筑物中，虽然一个警卫无法同时监视所有囚犯，但是由于采用了panopticon 设计理念，每个囚犯都不知道警卫是否在监视，因此始终会担心警卫在监视他。

信息来源：https://www.aqniu.com/threat-alert/73122.html

NSFOCUS

漏洞聚焦

Apache Druid 远程执行代码漏洞 (CVE-2021-25646)

一、漏洞概述

近日，绿盟科技监测到Apache发布安全通告，修复了一个Apache Druid远程执行代码漏洞（CVE-2021-25646）。由于Apache Druid能够执行嵌入在各种类型的请求中的用户提供的JavaScript代码，经过身份认证的攻击者可以构造恶意请求，使用当前Druid权限在目标系统上执行任意代码。

Apache Druid 是用Java编写的面向列的开源分布式数据存储，旨在快速获取大量事件数据，并在数据之上提供低延迟查询。

参考链接：

https://www.mail-archive.com/announce@apache.org/msg06335.html

二、影响范围

受影响版本

☐ Apache Druid < 0.20.1

不受影响版本

☐ Apache Druid 0.20.1

三、漏洞防护

3.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下载链接：https://github.com/apache/druid/releases

3.2 临时防护措施

若相关用户暂时无法进行升级操作，也可通过设置白名单访问的方式进行临时缓解。

Apache Shiro 权限绕过漏洞 (CVE-2020-17523)

一、漏洞概述

近日，绿盟科技监测到Apache Shiro官方发布安全更新，修复了一个新的权限绕过漏洞（CVE-2020-17523）。当Apache Shiro与Spring结合使用时，攻击者可以构造特定的HTTP请求绕过身份验证访问后台功能；目前漏洞细节已公开，请相关用户采取措施进行防护。

Apache Shiro是一个功能强大且易于使用的Java安全框架，功能包括身份验证、授权、加密和会话管理。使用Shiro的API，可以轻松地、快速地保护任何应用程序，范围从小型的移动应用程序到大型的Web和企业应用程序。

参考链接：

https://shiro.apache.org/security-reports.html

二、影响范围

受影响版本

☐ Apache Shiro < 1.7.1

不受影响版本

☐ Apache Shiro = 1.7.1

三、漏洞检测

3.1 人工检测

相关用户可通过版本检测的方式判断当前应用是否存在风险。

在config\pom.xml的version标签中查看当前使用的shiro版本号:

```
<!-- shiro start -->
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-core</artifactId>
    <version>1.2.5</version>
</dependency>
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-ehcache</artifactId>
    <version>1.2.5</version>
</dependency>
<dependency>
    <groupId>net.sf.ehcache</groupId>
    <artifactId>ehcache-core</artifactId>
    <version>2.4.8</version>
</dependency>
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-spring</artifactId>
    <version>1.2.5</version>
</dependency>
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-web</artifactId>
    <version>1.2.5</version>
</dependency>
<!-- end shiro -->
```

若版本在受影响范围内则可能存在安全风险。

四、漏洞防护

4.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下载链接：https://shiro.apache.org/download.html

Apache Tomcat Session 反序列化代码执行漏洞（CVE-2021-25329）

一、漏洞概述

3月1日，绿盟科技监测到Apache软件基金会发布安全通告，修复了一个通过会话持久性进行RCE的漏洞，此漏洞为CVE-2020-9484的补丁绕过，如果使用了Tomcat的session持久化功能，不安全的配置将导致攻击者可以发送恶意请求执行任意代码，成功利用此漏洞需要同时满足以下4个条件：

1）攻击者能够控制服务器上文件的内容和文件名称；

2）服务器PersistenceManager配置中使用了FileStore；

3）PersistenceManager中的sessionAttributeValueClassNameFilter被配置为“null”，或者过滤器不够严格，导致允许攻击者提供反序列化数据的对象；

4）攻击者知道使用的FileStore存储位置到攻击者可控文件的相对路径；

参考链接：

https://www.mail-archive.com/announce@apache.org/msg06386.html

二、影响范围

受影响版本

- ☐ Apache Tomcat 10.0.0-M1—10.0.0
- ☐ Apache Tomcat 9.0.0.M1—9.0.41
- ☐ Apache Tomcat 8.5.0—8.5.61
- ☐ Apache Tomcat 7.0.0—7.0.107

不受影响版本

- ☐ Apache Tomcat 10.x>=10.0.2
- ☐ Apache Tomcat 9.x>=9.0.43
- ☐ Apache Tomcat 8.x>=8.5.63
- ☐ Apache Tomcat 7.x>=7.0.108

注：此问题已在Tomcat 10.0.1、9.0.42和8.5.62中修复，但这些版本未通过发行。

三、漏洞检测

3.1 人工检测

1）从Apache Tomcat官网下载的安装包名称中会包含Tomcat的版本号，如果用户解压后没有更改Tomcat的目录名称，可以通过查看文件夹名称来确

定当前使用的版本。

如果解压后的Tomcat目录名称被修改过，或者通过Windows Service Installer方式安装，可使用软件自带的version模块来获取当前的版本。也可以进入Tomcat安装目录的bin目录，运行version.bat（Linux运行version.sh）后，可查看当前的软件版本号。

```
D:\Program Files\Apache Software Foundation\Tomcat 9.0\bin>version.bat
Using CATALINA_BASE:   "D:\Program Files\Apache Software Foundation\Tomcat 9.0"
Using CATALINA_HOME:   "D:\Program Files\Apache Software Foundation\Tomcat 9.0"
Using CATALINA_TMPDIR: "D:\Program Files\Apache Software Foundation\Tomcat 9.0\t
emp"
Using JRE_HOME:        "D:\Program Files\Java\jdk1.8.0_131"
Using CLASSPATH:       "D:\Program Files\Apache Software Foundation\Tomcat 9.0\b
in\bootstrap.jar;D:\Program Files\Apache Software Foundation\Tomcat 9.0\bin\tomc
at-juli.jar"
Server version: Apache Tomcat/9.0.5
Server built:   Feb 6 2018 21:42:23 UTC
Server number:  9.0.5.0
OS Name:        Windows 7
OS Version:     6.1
Architecture:   amd64
JVM Version:    1.8.0_131-b11
JVM Vendor:     Oracle Corporation
D:\Program Files\Apache Software Foundation\Tomcat 9.0\bin>
```

2）查看conf/context.xml文件或具体项目的server.xml文件中，是否存在以下<Manager>节点

```
context.xml
1
2  <Manager·className="org.apache.catalina.session.PersistentManager"·>
3      ·debug=0
4      ·saveOnRestart="true"
5      ·maxActiveSession="-1"
6      ·minIdleSwap="-1"
7      ·maxIdleSwap="-1"
8      ·maxIdleBackup="-1"
9      ·<Store·className="org.apache.catalina.session.FileStore"·directory="../session"·/>
10
11 //这里代表的是文件持久化.也可以自己实现Store
12 </Manager>
```

若当前版本在受影响范围内且在PersistenceManager配置中使用了FileStore，则可能存在安全风险。

四、漏洞防护

4.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下载链接：

版本号	下载地址
Apache Tomcat 10.0.2	https://tomcat.apache.org/download-10.cgi
Apache Tomcat 9.0.43	https://tomcat.apache.org/download-90.cgi
Apache Tomcat 8.5.63	https://tomcat.apache.org/download-80.cgi
Apache Tomcat 7.0.108	https://tomcat.apache.org/download-70.cgi

4.2 其他防护措施

若相关用户暂时无法进行升级操作，也可采用以下措施进行临时缓解：

禁止使用Session持久化功能FileStore，或者单独配置sessionAttributeValue ClassNameFilte的值来确保只有特定属性的对象可以被序列化与反序列化。

VMware 多个高危漏洞通告

一、漏洞概述

2月23日，绿盟科技监测到VMware官方发布安全通告，披露了vSphere Client、ESXi的两个高危漏洞。

CVE-2021-21972：vSphere Client（HTML5）在vCenter Server插件vRealize Operations中包含一个远程执行代码漏洞，CVSSv3评分9.8。受影响的vRealize Operations插件为默认安装。目前已有PoC公开，请尽快采取措施进行防护。

CVE-2021-21974：ESXi中使用的OpenSLP存在堆溢出漏洞，CVSSv3评分8.8。与ESXi处于同一网段中且可以访问427端口的攻击者可触发OpenSLP服务中的堆溢出问题，从而导致远程执行代码。

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

二、影响范围

CVE-2021-21972

受影响版本

- ☐ vCenter Server 7.0 < 7.0 U1c
- ☐ vCenter Server 6.7 < 6.7 U3l
- ☐ vCenter Server 6.5 < 6.5 U3n
- ☐ Cloud Foundation (vCenter Server) 4.X < 4.2
- ☐ Cloud Foundation (vCenter Server) 3.X < 3.10.1.2

不受影响版本

- ☐ vCenter Server 7.0 U1c
- ☐ vCenter Server 6.7 U3l
- ☐ vCenter Server 6.5 U3n
- ☐ Cloud Foundation (vCenter Server) 4.2
- ☐ Cloud Foundation (vCenter Server) 3.10.1.2

CVE-2021-21974

受影响版本

- ☐ ESXi 7.0 < 70U1c-17325551
- ☐ ESXi 6.7 < 670-202102401-SG
- ☐ ESXi 6.5 < 650-202102101-SG
- ☐ Cloud Foundation (ESXi) 4.X <4.2
- ☐ Cloud Foundation (ESXi) 3.X

不受影响版本

- ☐ ESXi 70U1c-17325551
- ☐ ESXi 670-202102401-SG
- ☐ ESXi 650-202102101-SG
- ☐ Cloud Foundation (ESXi) 4.2
- ☐ Cloud Foundation (ESXi) 3.X 热补丁KB82705

三、漏洞防护

3.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，对应产品版本的下载链接及文档如下：

产品版本	下载链接	操作文档
VMware ESXi 7.0 ESXi70U1c-17325551	https://my.vmware.com/group/vmware/patch	https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-esxi-70u1c.html
VMware ESXi 6.7 ESXi670-202102401-SG		https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-202102001.html
VMware ESXi 6.5 ESXi650-202102101-SG		https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-202102001.html
VMware vCloud Foundation 4.2	https://docs.vmware.com/en/VMware-Cloud-Foundation/4.2/rn/VMware-Cloud-Foundation-42-Release-Notes.html	
VMware vCloud Foundation 3.10.1.2	https://docs.vmware.com/en/VMware-Cloud-Foundation/3.10.1/rn/VMware-Cloud-Foundation-3101-Release-Notes.html	
vCenter Server 7.0.1 Update 1	https://my.vmware.com/web/vmware/downloads/details?downloadGroup=VC70U1C&productId=974	https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u1c-release-notes.html
vCenter Server 6.7 U3l	https://my.vmware.com/web/vmware/downloads/details?downloadGroup=VC67U3L&productId=742&rPId=57171	https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3l-release-notes.html
vCenter Server 6.5 U3n	https://my.vmware.com/web/vmware/downloads/details?downloadGroup=VC65U3N&productId=614&rPId=60942	https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3n-release-notes.html

3.2 临时防护措施

3.2.1 CVE-2021-21972

可参考官方临时修复建议（https://kb.vmware.com/s/article/82374）禁用vROPS插件：

1. 通过SSH远程连接到VCSA（或远程桌面连接到Windows VC）
2. 备份以下文件：

- /etc/vmware/vsphere-ui/compatibility-matrix.xml (vCSA)
- C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui (Windows VC)

3. 使用文本编辑器添加一行：

```
<Matrix>
    <pluginsCompatibility>
        ....
            <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
        ....
    </pluginsCompatibility>
</Matrix>
```

最终文件内容如下：

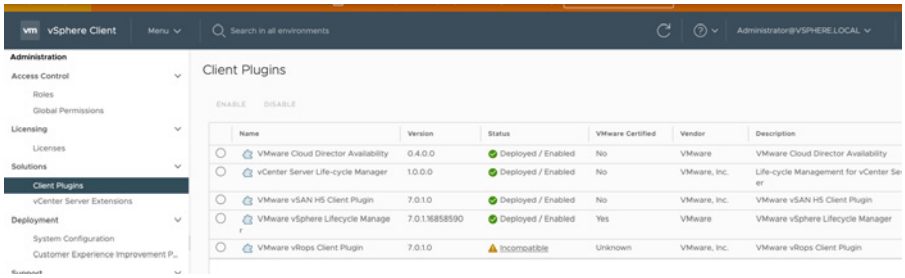
```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->
        <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

4. 重启vsphere-ui服务，命令：vmon-cli -r vsphere-ui。
5. 检查禁用情况：

访问https://<VC-IP-or-FQDN>/ui/vropspluginui/rest/services/checkmobregister，

该页面应显示404。

在VSphere Client页面的Solutions->Client Plugins中，VMware vRops Client Plugin插件应显示“incompatible”



3.2.2 CVE-2021-21974

可参考官方临时修复建议（https://kb.vmware.com/s/article/76372）禁用CIM服务器：

1. 使用以下命令在ESXi主机上停止SLP服务：/etc/init.d/slpd stop。仅当不使用SLP服务时，才可以停止该服务。可使用“esxcli system slp stats get”命令查看服务守护程序的运行状态。

2. 使用以下命令禁用SLP服务：esxcli network firewall ruleset set -r CIMSLP -e 0。

3. 使用以下命令保证此更改重启后依旧生效：chkconfig slpd off。

4. 使用以下命令检查是否重启后更改成功：chkconfig --list | grep slpd。若成功，输出应为：slpd off

微软 Exchange 多个高危漏洞

一、漏洞概述

3月2日，绿盟科技监测到微软发布Exchange Server的紧急安全更新，修复了7个相关漏洞，Exchange 服务端请求伪造漏洞（CVE-2021-26855）：攻击者能够发送任意HTTP请求并通过Exchange Server进行身份验证。Exchange反序列化代码执行漏洞（CVE-2021-26857）：具有管理员权限的攻击者可以在Exchange服务器上以SYSTEM身份运行任意代码。Exchange 任意文件写入漏洞（CVE-2021-26858/CVE-2021-27065）：经过身份验证的攻击者可以利用漏洞将文件写入服务器上的任何目录，可结合CVE-2021-26855进行组合攻击。及3个Exchange远程代码执行漏洞（CVE-2021-26412/CVE-2021-26854/CVE-2021-27078）。

目前微软已检测到在野利用，有部分漏洞的细节公开。请相关用户尽快采取措施进行防护。

参考链接：

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

二、影响范围

受影响版本

- ☐ Exchange Server 2019
- ☐ Exchange Server 2016
- ☐ Exchange Server 2013
- ☐ Exchange Server 2010

三、漏洞检测

3.1 本地扫描

用户可使用官方团队提供的Exchange Server运行状况检查脚本，判断查当前Exchange是否在漏洞影响范围，下载地址：

https://github.com/dpaulson45/HealthChecker#download

3.2 人工检测

用户可通过查看日志的方式检查服务器是否受到以上漏洞的攻击：

CVE-2021-26855：

可以通过以下Exchange HttpProxy日志进行检测：

%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProxy

通过以下Powershell命令可进行日志检测，并检查是否受到攻击：

```
Import-Csv -Path (Get-ChildItem -Recurse -Path “$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy” -Filter ‘*.log’).FullName | Where-Object { $_.AuthenticatedUser -eq ” -and $_.AnchorMailbox -like ‘ServerInfo~*/*’ } | select DateTime, AnchorMailbox
```

如果检测到了入侵，可以通过以下目录获取攻击者进行了哪些操作：

%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging

CVE-2021-26857：

可利用以下命令在应用程序事件中查询日志条目，并检查是否受到攻击。

```
Get-EventLog -LogName Application -Source “MSExchange Unified Messaging” -EntryType Error | Where-Object { $_.Message -like “*System.InvalidCastException*” }
```

CVE-2021-26858：

Exchange日志目录：C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog

可通过以下命令进行搜索，检查是否受到攻击：

```
findstr /snip /c:”Download failed and temporary file” “%PROGRAMFILES%\
```

```
Microsoft\Exchange Server\V15\Logging\OABGeneratorLog\*.log”
```

CVE-2021-27065:

Exchange日志目录：C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server

可通过以下powershell命令进行搜索，并检查是否遭到攻击:

```
Select-String -Path “$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\ECP\Server\*.log” -Pattern ‘Set-.+VirtualDirectory’
```

四、漏洞防护

4.1 补丁更新

目前微软官方已针对受支持的产品版本发布了修复该漏洞的安全补丁，建议受影响用户开启系统自动更新安装补丁进行防护。

注：由于网络问题、计算机环境问题等原因，Windows Update的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。右键点击Windows徽标，选择“设置(N)”，选择“更新和安全”-“Windows更新”，查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

针对未成功安装更新补丁的情况，可直接下载离线安装包进行更新，下载链接如下：

产品更新	补丁编号	补丁下载链接
Microsoft Exchange Server 2010 Service Pack 3	KB5000978	https://www.microsoft.com/en-us/download/details.aspx?id=102774
Microsoft Exchange Server 2013 Cumulative Update 23	KB5000871	https://www.microsoft.com/en-us/download/details.aspx?id=102775
Microsoft Exchange Server 2016 Cumulative Update 18	KB5000871	https://www.microsoft.com/en-us/download/details.aspx?id=102773
Microsoft Exchange Server 2016 Cumulative Update 19	KB5000871	https://www.microsoft.com/en-us/download/details.aspx?id=102772
Microsoft Exchange Server 2019 Cumulative Update 7	KB5000871	https://www.microsoft.com/en-us/download/details.aspx?id=102771

产品更新	补丁编号	补丁下载链接
Microsoft Exchange Server 2019 Cumulative Update 8	KB5000871	https://www.microsoft.com/en-us/download/details.aspx?id=102770

【注】：建议您在安装补丁前做好数据备份工作，避免出现意外。

4.2 防护建议

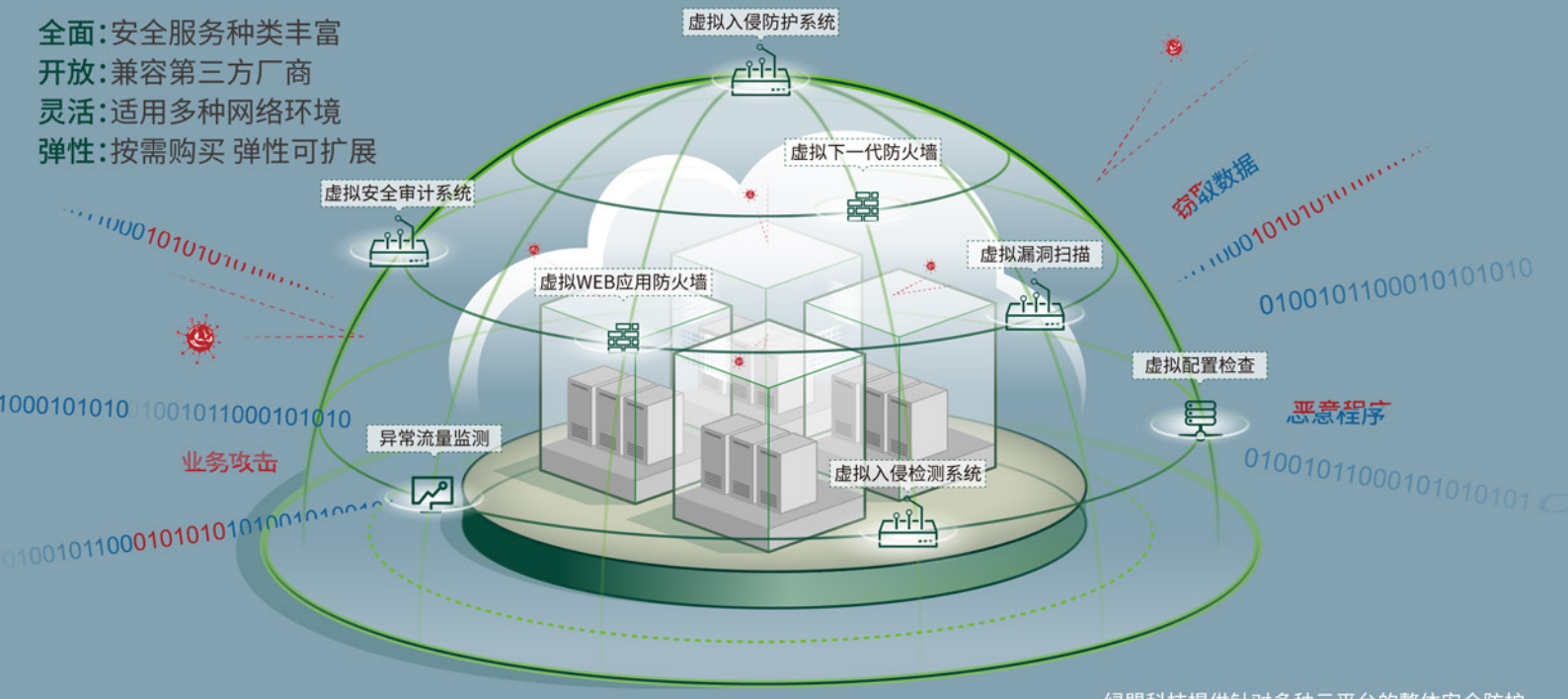
1、在未完成补丁修复之前，通过入侵检测设备重点监测Exchange服务器非法外连及对内端口扫描和蠕虫行为；

2、建议相关用户请勿打开来历不明的邮件，避免被攻击者利用漏洞在机器上执行恶意代码；

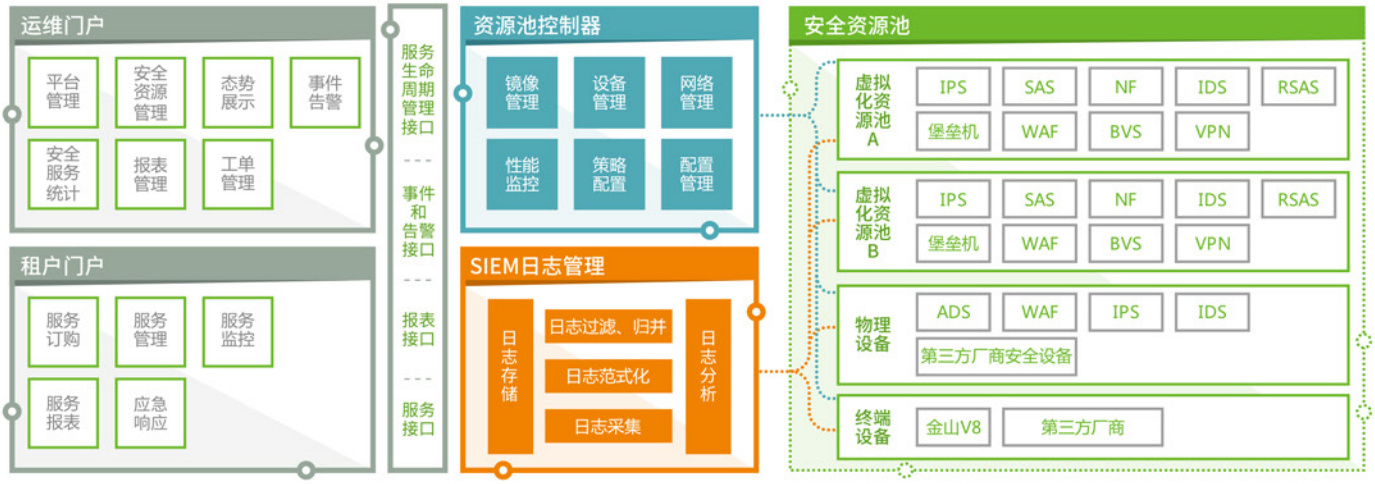
3、如果不能及时安装补丁，建议关注Exchange用户登录异常情况，清理僵尸账号、离职员工或供应商账号，以及重置登录异常的账户和弱口令账户密码，并使其满足较强的口令规范。

绿盟科技
云计算安全解决方案

全面:安全服务种类丰富
开放:兼容第三方厂商
灵活:适用多种网络环境
弹性:按需购买 弹性可扩展



绿盟科技提供针对多种云平台的整体安全防护



THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. 新的Masslogger特洛伊木马变种可过滤用户凭据

【概述】

臭名昭著的MassLogger Windows凭据窃取程序又回来了，它已升级为可以从Outlook，Chrome和即时通讯程序应用程序窃取凭据。

【参考链接】

https://securityaffairs.co/wordpress/114783/malware/masslogger-trojan.html

2. 利用格式错误URL前缀的钓鱼攻击激增6000%

【概述】

研究人员说，攻击者正在反钓鱼邮件URL中加反斜杠以逃避保护。

来自GreatHorn的研究人员报告说，他们已经观察到使用“格式错误的URL前缀”的攻击跳跃了近6,000%，从而逃避保护并发送看上去合法的网络钓鱼电子邮件。

【参考链接】

https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/

3. 黑客利用IT监控工具中心来监控多个法国公司

【概述】

与俄罗斯有关联的、由国家支持的攻击组织Sandworm和一项长达三年的秘密行动有关，该行动利用名为Centreon的IT监控工具攻击目标。

法国信息安全机构ANSSI在一份咨询报告中表示，根据研究，此次的攻击活动已经攻击了“几个法国公司”，该活动始于2017年底，持续到2020年，攻击特别影响了Web托管提供商。

【参考链接】

https://www.4hou.com/posts/MNEQ

4. 黑客滥用谷歌应用程序脚本窃取信用卡数据

【概述】

研究人员报告说，威胁行动者正在滥用Google的Apps Script商业应用开发平台来窃取电子商务网站客户提供的信用卡数据。

【参考链接】

https://securityaffairs.co/wordpress/114750/cyber-crime/googles-apps-script-magecart.html

5. 起亚确认遭DoppelPaymer勒索软件攻击的赎金高达两千万

【概述】

起亚汽车美国公司遭受了DoppelPaymer团伙的勒索软件攻击，要求提供2000万美元用于解密器，并且不得泄漏被盗的数据。

【参考链接】

https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/

6. 法国和乌克兰警方逮捕涉及Egregor勒索软件的犯罪团伙

【概述】

乌克兰和法国的执法部门联合开展行动，逮捕了一些与Egregor RaaS有联系的人，而不是主要的勒索软件帮派。

据法国媒体称，当局没有透露嫌疑人的姓名。嫌疑人正在与Egregor勒索软件运营商联系，并向他们提供后勤和财务支持。

【参考链接】

https://securityaffairs.co/wordpress/114590/cyber-crime/egregor-ransomware-arrests.html

7. Emotet尽管已被攻下，但仍然是最大的恶意软件威胁

【概述】

我们最新的2021年1月全球威胁指数显示，尽管国际警察行动在27日控制了该僵尸网络，但Emotet木马仍连续第二个月在顶级恶意软件列表中排名第一，影响了全球6%的组织。

【参考链接】

https://blog.checkpoint.com//blog.checkpoint.com/2021/02/11/january-2021s-most-wanted-malware-emotet-continues-reign-as-top-malware-threat-despite-takedown/

8. 美国起诉朝鲜黑客盗窃2亿美元

【概述】

美国司法部今天针对三名被指控与朝鲜政权合作实施网络犯罪攻击的人，发

起了起诉。其网络犯罪范围包括2014年对Sony Pictures的黑客攻击，2017年全球WannaCry勒索软件蔓延，并盗窃了大约2亿美元，并试图从全球的银行和其他受害者盗窃12亿多美元。

【参考链接】

https://krebsonsecurity.com/2021/02/u-s-indicts-north-korean-hackers-in-theft-of-200-million/

9. Chimera-一个PowerShell混淆脚本

【概述】

Chimera是一个PowerShell 脚本，旨在绕过AMSI和防病毒解决方案。它会触发AV的恶意PS1，并使用字符串替换和变量串联来逃避常见的检测签名。

【参考链接】

https://www.kitploit.com/2021/02/chimera-shiny-and-very-hack-ish.html

10. ScamClub malvertising团伙滥用WebKit浏览器零日漏洞

【概述】

恶意广告团伙ScamClub滥用了基于WebKit的浏览器中未修补的零日漏洞，以绕过安全措施并将用户从合法站点重定向到托管在线礼品卡欺诈的网站。

恶意广告活动最早于2020年6月发现，尽管该漏洞已在本月初发布的安全更新中得到解决，但仍在继续进行。

【参考链接】

https://securityaffairs.co/wordpress/114689/cyber-crime/scamclub-malvertising-webkit-zero-day.htm

11. 以蓝军视角跟踪和分析CANVAS攻击框架泄露事件

【概述】

3月3日，绿盟科技研究团队在对网络安全事件舆情监控中发现著名的商业渗透框架CANVAS系统源代码发生泄露，绿盟科技M01N蓝军研究团队第一时间对该事件进行了跟踪，快速分析了CANVAS的攻击框架、所涉及的漏洞和技术细节。

【参考链接】

https://mp.weixin.qq.com/s/eQ-KDMoirOwx-pFxUcNjtQ

12. 牛津大学COVID-19实验室被黑客攻击

【概述】

牛津大学研究生物学方法以对抗COVID-19的实验室已成为黑客进行网络攻击活动的目标。牛津大学发言人证实，被黑客入侵的该生物实验室系统不包含任何患者数据，并且不侵犯患者的机密性。

【参考链接】

https://www.welivesecurity.com/2021/02/26/oxford-university-covid19-laboratory-hack/

13. GenuGate防火墙关键身份绕过漏洞已修复

【概述】

总部位于德国的网络安全公司Genua已针对GenuGate防火墙中的严重缺陷迅速进行了修复。如果利用此漏洞，则本地攻击者可能会绕过身份验证措施，并以最高级别的特权登录到公司内部网络。

【参考链接】

https://threatpost.com/firewall-critical-security-flaw/164347/

14. PrismHR遭勒索软件攻击

【概述】

PrismHR是一家以帮助80,000多家小型企业管理工资、福利和人力资源的公司，该公司近日遭受了持续的勒索软件攻击，严重影响多项业务正常进行。

【参考链接】

https://krebsonsecurity.com/2021/03/payroll-hr-giant-prismhr-hit-by-ransomware/

15. Ryuk勒索软件新版本可进行蠕虫状的自我传播

【概述】

Ryuk勒索软件新版本能够在本地网络中通过SMB共享和端口扫描进行自我复制，并读取受感染设备的地址解析协议（ARP）表，该表存储了与计算机通信的任何网络设备的IP地址和MAC地址。

【参考链接】

https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/

16. 通用医疗服务公司(UHS)遭攻击后面临巨额损失

【概述】

在2020年9月-10月期间针对通用医疗服务公司（UHS）的网络攻击事件使该公司蒙受了高达6700万美元的损失，该公司是美国最大的医疗管理公司之一，报道指出该次网络攻击的罪魁祸首是Ryuk勒索软件。

【参考链接】

https://threatpost.com/post-cyberattack-universal-health-services-faces-67m-in-losses/164424/

17. Clop勒索软件团伙泄露从网络安全公司Qualys窃取的数据

【概述】

Clop勒索软件团伙利用了Accellion FTA服务器中的零日漏洞窃取网络安全公司Qualys的数据，并在其泄露站点上共享了被盗文件的截图信息，泄露的数据包括发票、采购订单、税单和扫描报告等，受到同样攻击的还有新南威尔士州的运输公司和庞巴迪公司。

【参考链接】

https://securityaffairs.co/wordpress/115250/data-breach/qualys-clop-ransomware.html

18. 2100万免费VPN用户数据遭泄露

【概述】

超过2100万移动VPN应用程序用户的详细凭证在网上出售，数据包括电子邮件地址、随机生成的密码字符串、付款信息以及属于三个VPN应用程序（SuperVPN、GeckoVPN和ChatVPN）用户的设备ID。

【参考链接】

https://blog.malwarebytes.com/cybercrime/privacy/2021/03/21-million-free-vpn-users-data-exposed/

19. Gafgyt新变体针对D-Link和物联网设备的攻击活动

【概述】

Gafgyt僵尸网络的新变种是依赖Tor通信的恶意软件，主要针对易受攻击的D-Link和物联网设备。Gafgyt是一个于2014年发现的僵尸网络，它因发动大规模分布式拒绝服务（DDoS）攻击而声名狼藉，新变种Gafgyt_tor为规避检测，使用Tor来隐藏其命令和控制（C2）通信，并对样本中的敏感字符串进行加密。

【参考链接】

https://threatpost.com/d-link-iot-tor-gafgyt-variant/164529/

20. 针对航空公司的供应链攻击活动

【概述】

总部位于瑞士的IT公司SITA，为全球90%的航空公司提供IT服务，近期该公司受到供应链攻击导致大量乘客信息遭泄露，已有马来西亚航空、新加坡航空、芬兰航空和新西兰航空受到此次攻击活动的影响。

【参考链接】

https://www.inforisktoday.com/supply-chain-attack-jolts-airlines-a-16123

21. 黑客入侵欧盟银行监管机构EBA的Exchange服务器

【概述】

欧盟银行监管机构EBA的Microsoft Exchange电子邮件系统遭黑客攻击，此次攻击活动疑似与HAFNIUM攻击组织有关。

【参考链接】

https://securityaffairs.co/wordpress/115396/data-breach/eba-microsoft-exchange-hacked.html

22. Emotet木马威胁活动供应链分析

【概述】

银行木马Emotet自2020年12月以来一直活跃，Emotet通常随网络钓鱼电子邮件一起发送，附带Word文档，Emotet攻击链中的步骤：a.Word文档已分发并在启用宏的情况下打开;b.运行VBScript宏以生成恶意的PowerShell脚本;c.恶意的PowerShell脚本将初始DLL二进制文件下载为加载程序;d.初始加载程序将删除后

续的DLL二进制文件，该二进制文件将进行自我更新;e.最终的DLL会窃取受害者的敏感数据，或者通过与C2服务器进行通信来进行进一步的攻击。

【参考链接】

https://unit42.paloaltonetworks.com/attack-chain-overview-emotet-in-december-2020-and-january-2021/

23. 加密挖矿活动针对QNAP NAS设备

【概述】

近期恶意加密货币活动中攻击者利用UnityMiner恶意软件针对QNAP Systems网络连接存储（NAS）设备，该设备关键固件可能存在未修补漏洞（CVE-2020-2506，CVE-2020-2507），根据QNAP设备映射，美国和中国的110万QNAP NAS用户受到严重影响，占全球感染总数的80%。

【参考链接】

https://threatpost.com/miner-campaign-targets-unpatched-qnap-nas/164580/

24. ZLoader恶意软件隐藏在加密的Excel文件中

【概述】

ZLoader是一种多用途木马，通常充当投递程序，在多阶段勒索软件攻击（例如Ryuk和Egregor）中传递基于Zeus的恶意软件。近期发现一起网络钓鱼攻击活动中，攻击者使用国税局税收和发票文件作为诱饵，将恶意软件ZLoader隐藏在加密的Excel文件中进行传播，旨在窃取敏感数据。

【参考链接】

https://www.inforisktoday.com/zloader-malware-hidden-in-encrypted-excel-file-a-16146

25. Verkada摄像头被黑客攻击

【概述】

黑客近期利用Verkada摄像头中的漏洞可远程访问客户摄像头，受害者包括汽车制造商Tesla、网络基础设施公司Cloudflare、身份和访问管理厂商Okta以及多家医院和监狱。Verkada总部位于加利福尼亚州圣马特奥，为众多组织管理和

维护150,000个可远程访问的监视摄像机。

【参考链接】

https://www.inforisktoday.com/startup-probes-hack-internet-connected-security-cameras-a-16155

26. OVH云数据中心被大火烧毁

【概述】

OVH是欧洲最大的托管服务提供商，也是世界第三大托管服务提供商，该云公司计算提供虚拟专用服务器，专用服务器和其他网络服务。近日一个OVH数据中心发生火灾，摧毁了一个数据中心，并使另外两个数据中心掉线；已确认受影响的EU服务器全部丢失。

【参考链接】

https://blog.malwarebytes.com/malwarebytes-news/2021/03/ovh-cloud-datacenter-destroyed-by-fire/

27. 数十万台Microsoft服务器持续被黑客入侵

【概述】

针对Microsoft Exchange服务器的攻击比想象的要糟糕很多，据数据显示，全球已有数十万台Microsoft服务器遭黑客攻击。

【参考链接】

https://www.forbes.com/sites/daveywinder/2021/03/06/warning-hundreds-of-thousands-of-microsoft-servers-hacked-in-ongoing-attack/?sh=63b15eb828e6

28. 针对Azure云平台用户的新攻击活动

【概述】

微软警告其Azure云平台的用户，黑客正在使用几种“living off the land”攻击技术来逃避安全措施，提升特权和部署加密矿工。

【参考链接】

https://www.inforisktoday.com/hackers-waging-living-off-land-attacks-on-azure-a-16158

29. REvil勒索软件使用DDoS攻击和语音呼叫向受害者施压

【概述】

REvil勒索软件运营商正在使用DDoS攻击，并向记者和受害人的商业伙伴发出语音呼叫，以迫使受害人支付赎金

【参考链接】

https://securityaffairs.co/wordpress/115345/cyber-crime/revil-ransomware-ddos-voice-calls.html

30. 新的Masslogger特洛伊木马变种可过滤用户凭据

【概述】

臭名昭著的MassLogger Windows凭据窃取程序又回来了，它已升级为可以从Outlook，Chrome和即时通讯程序应用程序窃取凭据。

【参考链接】

https://securityaffairs.co/wordpress/114783/malware/masslogger-trojan.html

31. 利用格式错误URL前缀的钓鱼攻击激增6000%

【概述】

研究人员说，攻击者正在反钓鱼邮件URL中加反斜杠以逃避保护。

来自GreatHorn的研究人员报告说，他们已经观察到使用“格式错误的URL前缀”的攻击跳跃了近6,000%，从而逃避保护并发送看上去合法的网络钓鱼电子邮件。

【参考链接】

https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/

32. 黑客利用IT监控工具中心来监控多个法国公司

【概述】

与俄罗斯有关联的、由国家支持的攻击组织Sandworm和一项长达三年的秘密行动有关，该行动利用名为Centreon的IT监控工具攻击目标。

法国信息安全机构ANSSI在一份咨询报告中表示，根据研究，此次的攻击活

动已经攻击了“几个法国公司”，该活动始于2017年底，持续到2020年，攻击特别影响了Web托管提供商。

【参考链接】

https://www.4hou.com/posts/MNEQ

33. 黑客滥用谷歌应用程序脚本窃取信用卡数据

【概述】

研究人员报告说，威胁行动者正在滥用Google的Apps Script商业应用开发平台来窃取电子商务网站客户提供的信用卡数据。

【参考链接】

https://securityaffairs.co/wordpress/114750/cyber-crime/googles-apps-script-magecart.html

34. 起亚确认遭DoppelPaymer勒索软件攻击的赎金高达两千万

【概述】

起亚汽车美国公司遭受了DoppelPaymer团伙的勒索软件攻击，要求提供2000万美元用于解密器，并且不得泄漏被盗的数据。

【参考链接】

https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/

35. 法国和乌克兰警方逮捕涉及Egregor勒索软件的犯罪团伙

【概述】

乌克兰和法国的执法部门联合开展行动，逮捕了一些与Egregor RaaS有联系的人，而不是主要的勒索软件帮派。

据法国媒体称，当局没有透露嫌疑人的姓名。嫌疑人正在与Egregor勒索软件运营商联系，并向他们提供后勤和财务支持。

【参考链接】

https://securityaffairs.co/wordpress/114590/cyber-crime/egregor-ransomware-arrests.html

36. Emotet尽管已被攻下，但仍然是最大的恶意软件威胁

【概述】

我们最新的2021年1月全球威胁指数显示，尽管国际警察行动在27日控制了该僵尸网络，但Emotet木马仍连续第二个月在顶级恶意软件列表中排名第一，影响了全球6%的组织。

【参考链接】

https://blog.checkpoint.com//blog.checkpoint.com/2021/02/11/january-2021s-most-wanted-malware-emotet-continues-reign-as-top-malware-threat-despite-takedown/

37. 美国起诉朝鲜黑客盗窃2亿美元

【概述】

美国司法部今天针对三名被指控与朝鲜政权合作实施网络犯罪攻击的人，发起了起诉。其网络犯罪范围包括2014年对Sony Pictures的黑客攻击，2017年全球WannaCry勒索软件蔓延，并盗窃了大约2亿美元，并试图从全球的银行和其他受害者盗窃12亿多美元。

【参考链接】

https://krebsonsecurity.com/2021/02/u-s-indicts-north-korean-hackers-in-theft-of-200-million/

38. Chimera-一个PowerShell混淆脚本

【概述】

Chimera是一个PowerShell 脚本，旨在绕过AMSI和防病毒解决方案。它会触发AV的恶意PS1，并使用字符串替换和变量串联来逃避常见的检测签名。

【参考链接】

https://www.kitploit.com/2021/02/chimera-shiny-and-very-hack-ish.html

39. ScamClub malvertising团伙滥用WebKit浏览器零日漏洞

【概述】

恶意广告团伙ScamClub滥用了基于WebKit的浏览器中未修补的零日漏洞，以绕过安全措施并将用户从合法站点重定向到托管在线礼品卡欺诈的网站。

恶意广告活动最早于2020年6月发现，尽管该漏洞已在本月初发布的安全更新中得到解决，但仍在继续进行。

【参考链接】

https://securityaffairs.co/wordpress/114689/cyber-crime/scamclub-malvertising-webkit-zero-day.htm

让安全更有效
绿盟科技安全服务

专业|灵活|高效

咨询服务
安全规划
合规咨询
信息安全管理体系咨询
应急体系建设
……

可管理安全服务
远程安全运维
全评估/测试服务
安全基线服务
应急响应
……

安全评价
外部检查辅导
安全指标体系度量
……

安全研究
渗透测试
源代码审计
业务安全测试
漏洞挖掘
……

教育培训
安全技能培训
安全意识教育
……

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

安全月报

绿盟科技金融事业部出品

主办/绿盟科技金融事业部
地址/北京市海淀区北洼路4号益泰大厦3层
邮编/100089
电话/010-59610688-1159
传真/010-59610689
网站/www.nsfocus.com
客户支持热线/400-818-6868
股票代码/300369
月报电子版下载/https://www.nsfocus.com.cn/html/7/20/34/