www.darkowl.com
July, 2021

ESTABLISHING FOOTHOLDS: EXAMINING THE CURRENT RANSOMWARE-AS-A-SERVICE ECOSYSTEM

This paper examines how ransomware-as-a-service (RaaS) gangs have morphed into an ever-evolving and elusive threat, deploying increasingly sophisticated malware in tandem with advanced deception methodologies to evade detection, and maintain persistent access to victim networks and compromised devices. Most notably, research and observations from the darknet point to the likelihood that the recent string of ransomware attacks are not as random as they would want us to perceive, but in fact are indicative of a more organized and elaborate cyber stratagem.

To couple operational evidence with telemetry from the darknet, we spoke directly to security researchers, exploit experts, and incident responders to foster a greater collaborative understanding of the RaaS criminal industry. We discovered how RaaS groups utilize backdoors to maintain persistent access to their victims during a campaign and potentially long after ransom payment is applied and decryption keys released.

What emerged as a result of this research is an increasingly complex picture of the RaaS criminal ecosystem that merits considerable dialogue across all echelons of information security research, organizational cybersecurity departments, public sector information security and end point protection providers, as well as national cybersecurity policy makers. While we may not be able to predict the next victim, we should reflect on exactly where each of the RaaS gangs have been, what operational tactics they favor, and how the tools they are currently using or are actively developing in their terminals can help shape, and possibly predict, the next technical evolutionary steps of the ransomware/extortion-as-service threat model.

ESTABLISHING FOOTHOLDS: A LOOK AT RAAS FROM 5,280 FEET

The pace and intensity of tracking ransomware threat actors on the darknet continues to escalate, with RaaS groups constantly morphing through intentional rebranding and ever-evolving tactics, techniques, and procedures (TTPs). Tor onion services, which are predictably unstable, present a challenge like no-other, especially when identities and originating locations are obfuscated through Tor darknet protocols and encrypted one-to-one communications like qTox.

Despite these challenges, DarkOwl has been following the trends closely and collecting any-and-all data RaaS groups share publicly on their services and across darknet forums and marketplaces.

While it’s easy to get caught up in the neverending day-to-day surge of ransomware victims’ announcements and other daily darknet drama, it’s worthwhile to consider the “bigger picture” that is often lost in reactionary media coverage and flurry of external requests for information (RFIs).

By stepping out of the tactical mire, one can begin to see the potential strategic implications and ramifications of potential persistent footholds established by the elusive darknet RaaS criminal ecosystem.

TABLE OF CONTENTS

AN EVER-GROWING LIST OF RANSOMWARE VICTIMS

As part of the investigative effort centered around ransomware, threat research organizations have identified and reported on several thousand victims across the publicly known RaaS threat actors, detailing the most frequently attacked industries for each group. In 2020, Maze and Egregor – and also likely affiliated threat actors – conducted the largest number of attacks and retail and healthcare sectors in the United States were the most frequently targeted across all groups. [1]

In the first half of 2021, RaaS operations skyrocketed with a drastic increase in ransomware attacks around the globe – where publicly reported attacks across 34 known unique operators in the darknet far surpassed those observed in the entire 2020 year.

Unfortunately, such reports are estimates at best. This is in part due to the fact that many RaaS groups do not actually publish the names of every victim, as some victims pay the ransom fee upfront to avoid being publicly mentioned on the RaaS group's Tor service. In other cirumstances, certain controversial or highly publicized attacks garner enough attention from law enforcement or the news media that the victims are often omitted from the public-facing blog, or taken abruptly by the RaaS operators. [2]

According to the the total numbers reported for 2021, the Conti ransomware gang dominated the number of total volume of attacks, followed closely by REvil (aka Sodinokibi). Maze shut down its operations in the fall of 2020, possibly rebranding and operating as Egregor through the end of 2020. Until late July when they appeared to cease all operations, REvil continued to be an instrumental group across the RaaS community with a significant volume of affiliates launching attacks using their specific version of ransomware in exchange for a percentage of the ransom payment obtained.

Since RaaS groups rarely retire, it is likely that REvil has merely rebranded and will continue to operate under a new marquee.

IS IT ALL RANDOM?

While RaaS groups like DarkSide state they would not attack healthcare, medical, or educational institutions – despite hitting victims such as primehealthservices.com in March 2021 – there have been over three dozen victims (at the very least) in the health and medical industries extorted across other RaaS operators. DarkSide disappeared, or likely rebranded their operations, earlier this year after the critical infrastructure attack that shutdown 5,500 miles of Colonial's gas pipeline in Alpharetta, Georgia. As recently as mid-May, Ireland's National Health Service suffered a catastrophic ransomware attack forcing it to shut down its entire network rendering patients unable to schedule appointments and doctors unable to review records.

Since we cannot trust the word of a random RaaS group's spokesperson regarding their primary target victim by industry, we should neither believe their professions that all of this is merely a personal economical endeavor for opportunistic financial gain. For example, in addition to critical infrastructure and public utilities, DarkOwl has also observed an uptick in the number of recent strategic military targets mentioned in RaaS press releases – most notably U.S. nuclear facilities and technical software contractor, Sol Oriens in Albuquerque and the German military services contractor EDS Dienstleistungsgruppe are both victims announced by REvil in early-June 2021.

Last summer, a service contractor providing technical support to the Minuteman intercontinental-ballistic missile (ICBM) program known as Westtech International – coincidentally also located in Albuquerque – was compromised and information stolen for extortion by Doppelpaymer ransomware. [3,4]

1. https://www.flashpoint-intel.com/blog/ransomware-retrospective-analyzing-1100-attacks-from-2020/
2. DarkTracer Table: https://drive.google.com/file/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3/view
3. https://news.sky.com/story/hackers-steal-secrets-from-us-nuclear-missile-contractor-11999442
4. https://www.bankinfosecurity.com/blogs/ransomware-gang-goes-nuclear-hitting-us-weapons-contractor-p-3056

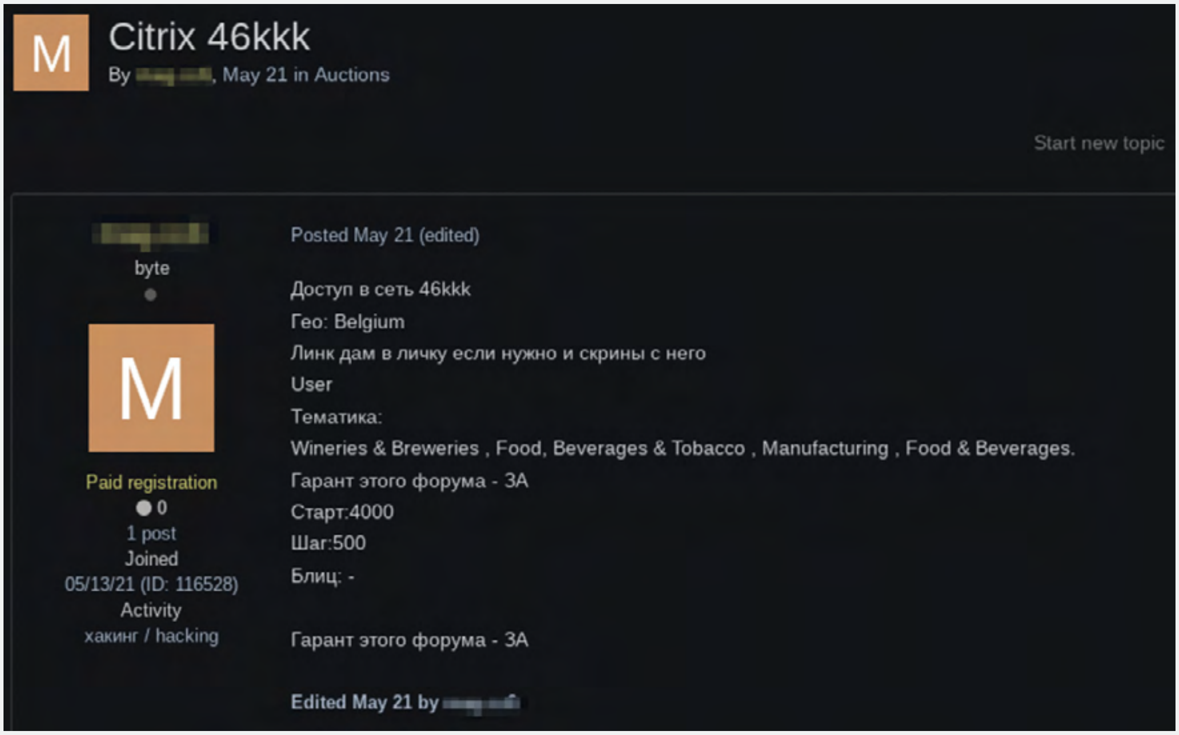
UNREGULATED SOFTWARE TOOLS BEHIND CYBER CHAOS

As the debate regarding the true motivation behind these increasingly dangerous and critical ransomware attacks continues, most all cybersecurity researchers will agree that the strategic employment of sophisticated software tools to penetrate, laterally move around a victim's network, and extract sensitive organizational information, prior to encrypting the network for ransom, is what drives continued success of such unparalleled tactical cyber offensive operations. The RaaS business model offers its affiliates the opportunity to rent ransomware for as little as $500 USD to $2,000 USD per year, meaning not only is there no real financial barrier to entry into the market, but that elite malware development skills are no longer required for conducting a successful campaign.

Likewise, many RaaS operators utilize a network of freelance darknet 'consultants' to fill in their capability gaps, such as penetrating testing services (i.e. network breach), to assist in the successful data extortion and deployment of the ransomware variant.

The initial attack vectors still rely primarily on a mixture of malware phishing campaigns, unpatched remote vulnerabilities and credential stuffing with exposed authentication parameters leaked on the darknet.

Freelance cybercriminals across darknet forums readily sell network credentials en masse. In recent months, Citrix vulnerabilities seem to be the most frequently mentioned platform. This is in contrast to last summer, where Pulse and F5 were more popularly discussed. These datasets are potential starting points for victim selection by industry and location.



Citrix 46kkk

By [redacted], May 21 in Auctions

Start new topic

[redacted]
byte

Paid registration
● 0
1 post
Joined
05/13/21 (ID: 116528)
Activity
хакинг / hacking

Posted May 21 (edited)

Доступ в сеть 46kkk
Гео: Belgium
Линк дам в личку если нужно и скрины с него
User
Тематика:
Wineries & Breweries , Food, Beverages & Tobacco , Manufacturing , Food & Beverages.
Гарант этого форума - 3А
Старт:4000
Шаг:500
Блиц: -

Гарант этого форума - 3А

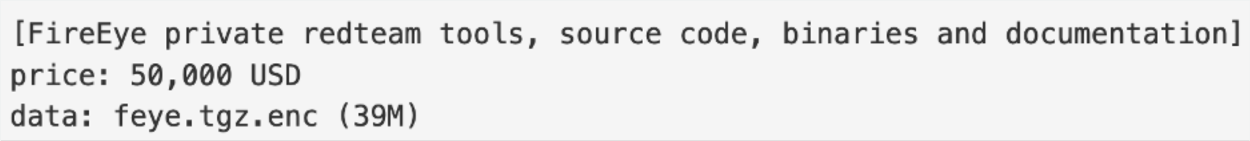
Edited May 21 by [redacted]

Figure 1: Darknet forum user offers over 46,000 Citrix credentials at an online auction for $4,000 USD.

[1] https://threatit.com/articles/tools-stolen-from-fireeye-could-hack-millions-of-devices/

Of additional concern is the leak of FireEye's network penetration toolkit compromised by Solarwinds/ SUNBURST related cyberattacks conducted back in December 2020. The tools stolen from FireEye target 16 known vulnerabilities in products across eight popular commercial software vendors: Pulse Secure, Microsoft, Fortinet, Adobe, Atlassian, Citrix, Zoho and Confluence. [1]

A surface website known as solarleaks.net emerged in early 2021 allegedly offering to sell data stolen during the SolarWinds campaign including the FireEye toolkit for $50,000 USD. Users of a popular darknet forum openly discussed this listing, many calling it scam, while others criticized the capitalistic approach stating, " смерть барыгам, держите бесплатно " which translates to "death to the dealers, keep it free." [1,2]

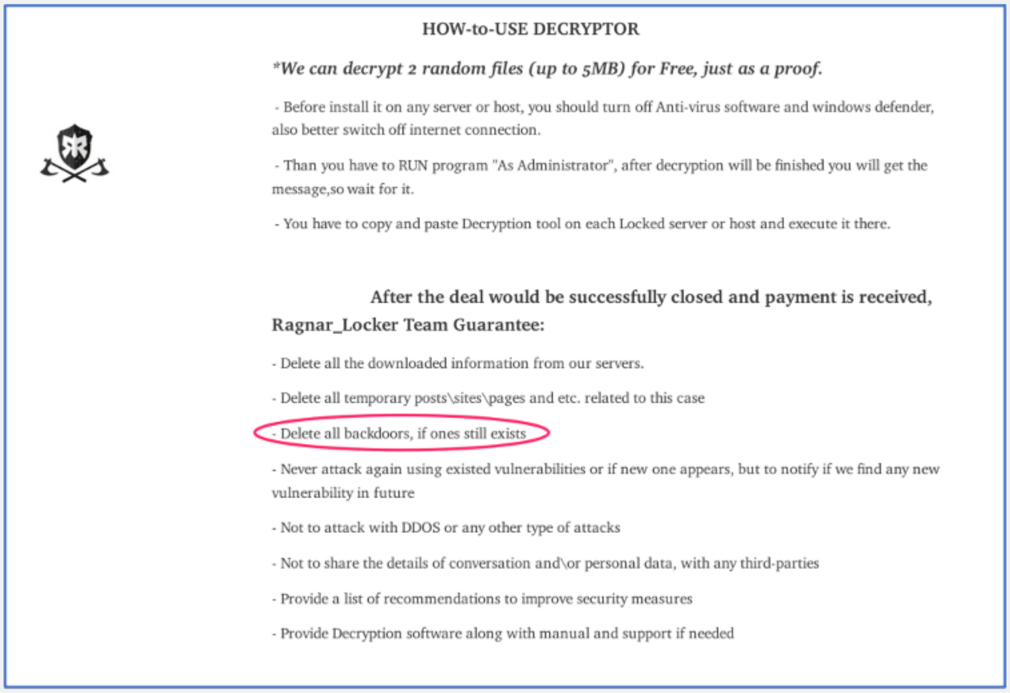


```
[FireEye private redteam tools, source code, binaries and documentation]
price: 50,000 USD
data: feye.tgz.enc (39M)
```

Knowing such highly sophisticated commercial tools are readily available on the darknet, what happens once access to a network is established by a RaaS criminal gang?

ESTABLISHING NETWORK FOOTHOLDS BY HIDING IN PLAIN SIGHT

We believe that darknet RaaS operators readily create network persistence by employing various levels of system 'backdoors' in ransomware campaigns against its victims and will continue this practice with increasingly sophisticated methods. We have observed RaaS operators on the darknet state out-right that they will "delete all backdoors, if one still exists" upon ransom payment and have observed other RaaS operators speculate about the scale of the volume of backdoors that "might exist" across victims worldwide.



HOW-to-USE DECRYPTOR

**We can decrypt 2 random files (up to 5MB) for Free, just as a proof.*

- Before install it on any server or host, you should turn off Anti-virus software and windows defender, also better switch off internet connection.

- Than you have to RUN program "As Administrator", after decryption will be finished you will get the message,so wait for it.

- You have to copy and paste Decryption tool on each Locked server or host and execute it there.

After the deal would be successfully closed and payment is received, Ragnar_Locker Team Guarantee:

- Delete all the downloaded information from our servers.

- Delete all temporary posts\sites\pages and etc. related to this case

- Delete all backdoors, if ones still exists

- Never attack again using existed vulnerabilities or if new one appears, but to notify if we find any new vulnerability in future

- Not to attack with DDOS or any other type of attacks

- Not to share the details of conversation and\or personal data, with any third-parties

- Provide a list of recommendations to improve security measures

- Provide Decryption software along with manual and support if needed

Figure 2: Ragnar_Locker Team's Terms and Conditions for Decryptor Use and Ransom Payment

[1] https://xopero.com/blog/en/2021/01/18/solarleaks-a-new-chapter-in-the-solarwinds-data-breach
[2] https://www.bleepingcomputer.com/news/security/solarleaks-site-claims-to-sell-data-stolen-in-solarwinds-attacks/

Incident responders have noted increased use of malicious backdoors by RaaS operators to establish a foothold in the compromised network. Cyberattacks conducted by novice cyber criminals are focused on maximizing malicious impact with an extremely short dwell time, i.e. a "get-in-and-get-out" type approach that doesn't easily lend itself to persistence. But, a modest degree of persistence is necessitated for RaaS groups who are conducting double extortion-type campaigns against their victims, where harvesting large volumes of sensitive corporate data from the network provides leverage against the ransomware victim. On the other hand, persistence would be absolutely vital for any sort of nation-state level cyber espionage activity.

Cobalt Strike has been frequently observed in successful RaaS operations and discussed widely across darknet forums. Cobalt Strike is a well-known software adversary emulation environment "designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors" traditionally utilized by red-teams in penetration tests and vulnerability assessments. Cobalt Strike has multiple methods to obscure detection by traditional desktop and corporate AV platforms: shellcode obfuscation and malleable command and control (C2). One dynamic link library (dll) stager involved Cobalt Strike hiding its payload shellcode over a named pipe, requiring the anti-virus emulate named pipes in order to detect the malicious executable. [1]

Cobalt Strike is capable of further detection evasion by mimicking HTTP requests for other popular web services such as Amazon, Google, etc, in sending data and receiving encrypted instructions from the Cobalt Strike Beacon C2 botnet. Fortunately, incident responders generally rely on IP addresses to detect malicious network activity, thus such falsified HTTP traffic should be easily detected by automated network monitoring software, such as the Real Intelligence Threat Analytics (RITA) project by Black Hills Information Security that has built-in automated beaconing detection. [2]

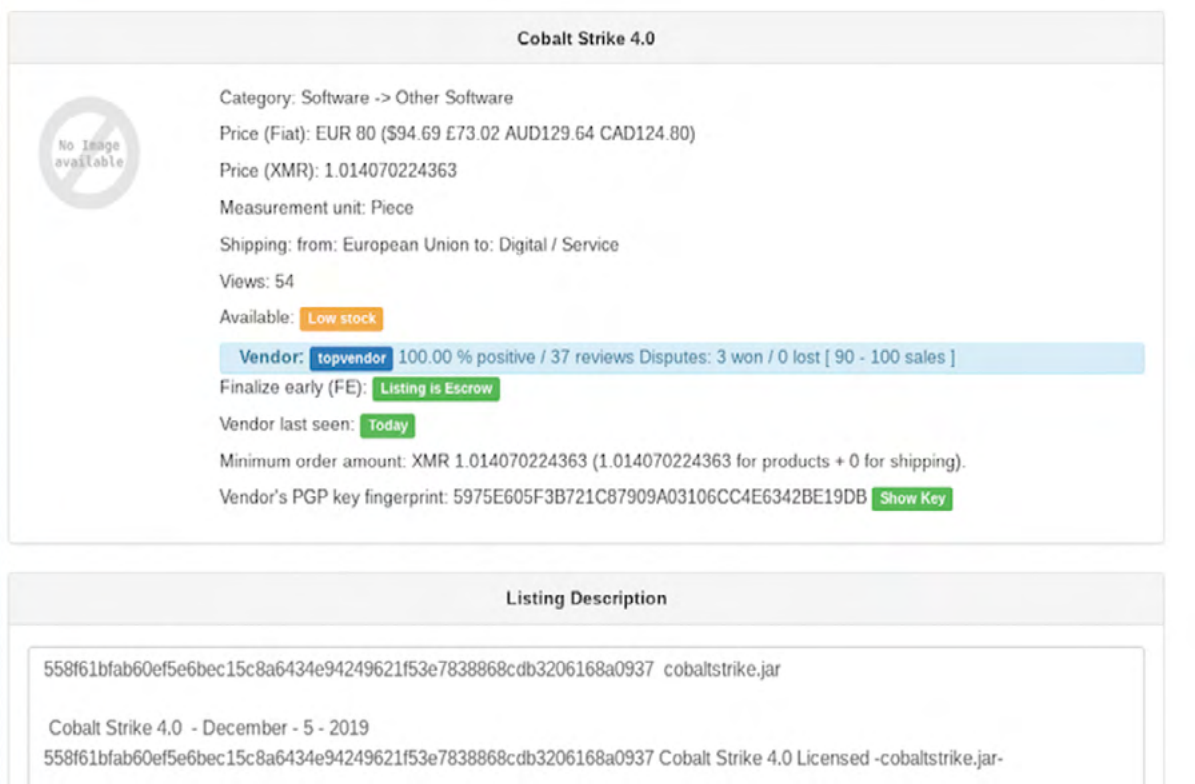
Some threat actors have also levied installations of F-Secure Labs' Custom Command and Control (C3) framework, to relays configured to proxy C2 communications through the Slack API, most likely to obfuscate traffic to and from Cobalt Strike Beacon. Detecting such advanced obscuration and network traffic deception methods requires excruciating discipline and rigorous manual network traffic log monitoring, which small business units and non-profit organizational IT departments likely do not have the bandwidth nor resources to perform. [3]

Cobalt Strike has seen increased adoption by RaaS actors and nation-state hacking campaigns. Open-source reporting from last year indicated that Chinese hackers sponsored by the Chinese government have been actively using Cobalt Strike to enable backdoor access to a number of compromised networks and information systems for the deployment of additional tools on the network in the future. Detecting and seizing the C2 servers at the heart of such malicious state-sponsored and criminal-gang orchestrated campaigns becomes a time-consuming process for threat hunters and incident responders.

> "Incident responders like myself have detected hundreds of Cobalt Strike Beacon servers around the world facilitating command and control functions for several ransomware operators.
>
> There are unfortunately not enough resources around the community to thoroughly investigate and take down all these servers. Besides, as soon as one is taken down, another Beacon server comes online elsewhere"
>
> - Ryan Chapman, Security Services Incident Response Consultant for BlackBerry

[1] https://blog.nviso.eu/2021/04/26/anatomy-of-cobalt-strike-dll-stagers/
[2] https://www.blackhillsinfosec.com/projects/rita/
[3] https://thestack.technology/from-c2-to-c3/

It will come as no surprise that Cobalt Strike is highly coveted and readily available for purchase on the darknet across marketplaces and even from individuals on hacking forums. Recently, a darknet forum user expressed keen interest in obtaining a license key required for successful employment of Cobalt Strike – requesting a key in exchange for upwards of $2K USD in payment, a budget slightly under the commercial-off-the-shelf (COTS) price of $3,500 USD for a new annual license and $2,585 USD for a license renewal.



Cobalt Strike 4.0

Category: Software -> Other Software

Price (Fiat): EUR 80 ($94.69 £73.02 AUD129.64 CAD124.80)

Price (XMR): 1.014070224363

Measurement unit: Piece

Shipping: from: European Union to: Digital / Service

Views: 54

Available: Low stock

Vendor: topvendor 100.00 % positive / 37 reviews Disputes: 3 won / 0 lost [90 - 100 sales]

Finalize early (FE): Listing is Escrow

Vendor last seen: Today

Minimum order amount: XMR 1.014070224363 (1.014070224363 for products + 0 for shipping).

Vendor's PGP key fingerprint: 5975E605F3B721C87909A03106CC4E6342BE19DB

Listing Description

558f61bfab60ef5e6bec15c8a6434e94249621f53e7838868cdb3206168a0937 cobaltstrike.jar

Cobalt Strike 4.0 - December - 5 - 2019
558f61bfab60ef5e6bec15c8a6434e94249621f53e7838868cdb3206168a0937 Cobalt Strike 4.0 Licensed -cobaltstrike.jar-

Figure 3: Darknet Market Advertisement for Cobalt Strike 4.0 Listed for Sale

NON-BEACON BACKDOORS

Another backdoor identified during the DarkSide attack on the Colonial Pipeline includes what security researchers call SMOKEDHAM. The SMOKEDHAM backdoor consists of custom PowerShell code, served up via a malicious URL (e.g. a DarkSide used the Shopify e-commerce platform for the Colonial attack), which once installed is capable of keylogging, capturing screenshots, and executing arbitrary .NET commands on the Windows operating system. [1]

Other backdoors, likely created by initial access brokers (IABs) responsible for garnering access to the target network, consist of persistent unauthorized remote desktop protocol (RDP) sessions to an attacker-controlled server hosted on the Tor darknet used to further conceal the origins of the attack. Tor services on the victim machine are required to maintain the RDP session, as such the RaaS operators renamed processes to match those commonly observed on Windows, used the Non-Sucking Service Manager (nssm.exe) to install Tor as a service on the victim machine, and created custom services.bat batch files to keep the Tor client running. [2]

[1] https://community.riskiq.com/article/fdf74f23
[2] https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access

Some persistence involves setting up a C2 communications link via task scheduling once a threat actor has gained access to a network domain. Threat actors behind the Pysa/Mespinoza ransomware variant installed the offensive security tool (OST) known as Kodiac advertised as a post-exploitation memory persistent rootkit for network penetration testers. Once Kodiac was installed on the victim network, threat actors simply setup a scheduled task to execute a malicious HTML application (HTA) file that facilitated C2 communications at logon so even after the machine was rebooted, the persistence subsists.

Incident responders have an assortment of methods to identify such rogue schtasks (task scheduler jobs in Windows). Least frequency occurrence (LFO) analysis, also known as stack counting, is one of many techniques available to detect malicious communications traffic, but rarely used in automated detection which as of late is required due the sheer volume of noise created by increased network traffic.

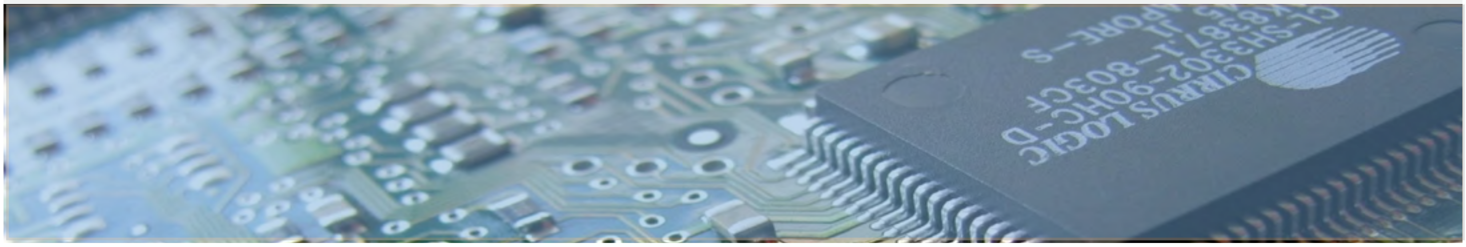
“We regularly see scheduled tasks, services, and run keys along with Cobalt Strike Beacons, oh so often. We also see WMI [Windows Management Instrumentation] consumers here and there, but it’s generally a ‘darn scheduled task or service’, something ever-so simple that these RaaS groups are utilizing,” Chapman added.

Operating-system level backdoors, like shellcode and task schedulers, are easily mitigated post-ransomware attack through wiping the data hard drives of all compromised devices on the network and loading a clean backup, presumably before the initial network compromise occurred and backdoors could have been installed. Unfortunately, many IT departments will attempt to restore access as quickly as possible - for example when JBS’s ransomware attack impacted the world meat supply chain - with the most recent data generated by its organizational users. Not properly cleaning networks of potential backdoors could be one of many reasons behind a recent CBS news report suggesting 80% of ransomware victims suffer repeat attacks. [1]

GOING DEEPER THAN THE OPERATING SYSTEM

Below the OS malware, such as firmware and BIOS/UEFI (Unified Extensible Firmware Interface) exploits, are malicious threat vectors that would provide a level of persistence that could not be remediated with simple hard drive re-imaging or fresh operating systems reinstalls. Firmware malware involves an attacker appending malicious machine-level codes to device firmware code that would be undetectable by traditional anti-virus and security protection measures such as checksum validations. Remediation would require physical flashing equipment firmware and possible involvement of the device manufacturer. BIOS/UEFI malware modifies the boot record with what is known as modified “bootkits” that could allow an attacker to control how the operating system starts up or even directly modify the OS to gain complete control over the system and subvert higher-layer network and system security controls.

Security researchers at Eclypsium have recently observed the TrickBot malware, traditionally utilized alongside banking industry attacks but recently adapted for use in RaaS campaigns, performing firmware vulnerability reconnaissance in the wild.



[1] https://www.msn.com/en-us/news/us/80percent-of-ransomware-victims-suffer-repeat-attacks-new-report-says/ar-AAL5s7o

> "Something that nearly all publicly-known UEFI-targeted attacks in the wild have in common, is that they all leverage existing, off-the-shelf OSS tools to facilitate the attack. Examples include the MossaicRegressor campaign, that leveraged the Vector-EDK UEFI implant tooling from Hacking Team. This is a fully documented (down to the SOP level), public toolkit that any threat actor, researcher or red-teamer can leverage in an attack to target the UEFI, and it's been public for nearly 7 years.
>
> Another example that was found to be in use by the Russian GRU as well as the infamous "TrickBoot" module of Trickbot actors, is the use of drivers that exist as part of the "RWEverything" open source project. These signed drivers, trusted by the OS, are powerful tools that allow attackers to implant, or brick, the BIOS/UEFI. Some attacks even leverage the OSS CHIPSEC project to help enumerate vulnerabilities in firmware that can then be easily exploited.
>
> Finally, the UEFI is not the only firmware vector that actors target. Equally common is the BMC via the IPMI protocol...another way to subvert the rest of the entire security stack and OS, by diving underneath it in order to persist indefinitely. There are many more beyond, including peripherals, HDD firmware, IOT devices, and even critical appliances like VPNs, File Transfer Devices and Firewall firmware."
>
> - Scott Scheferman, Office of the CTO, Eclypsium

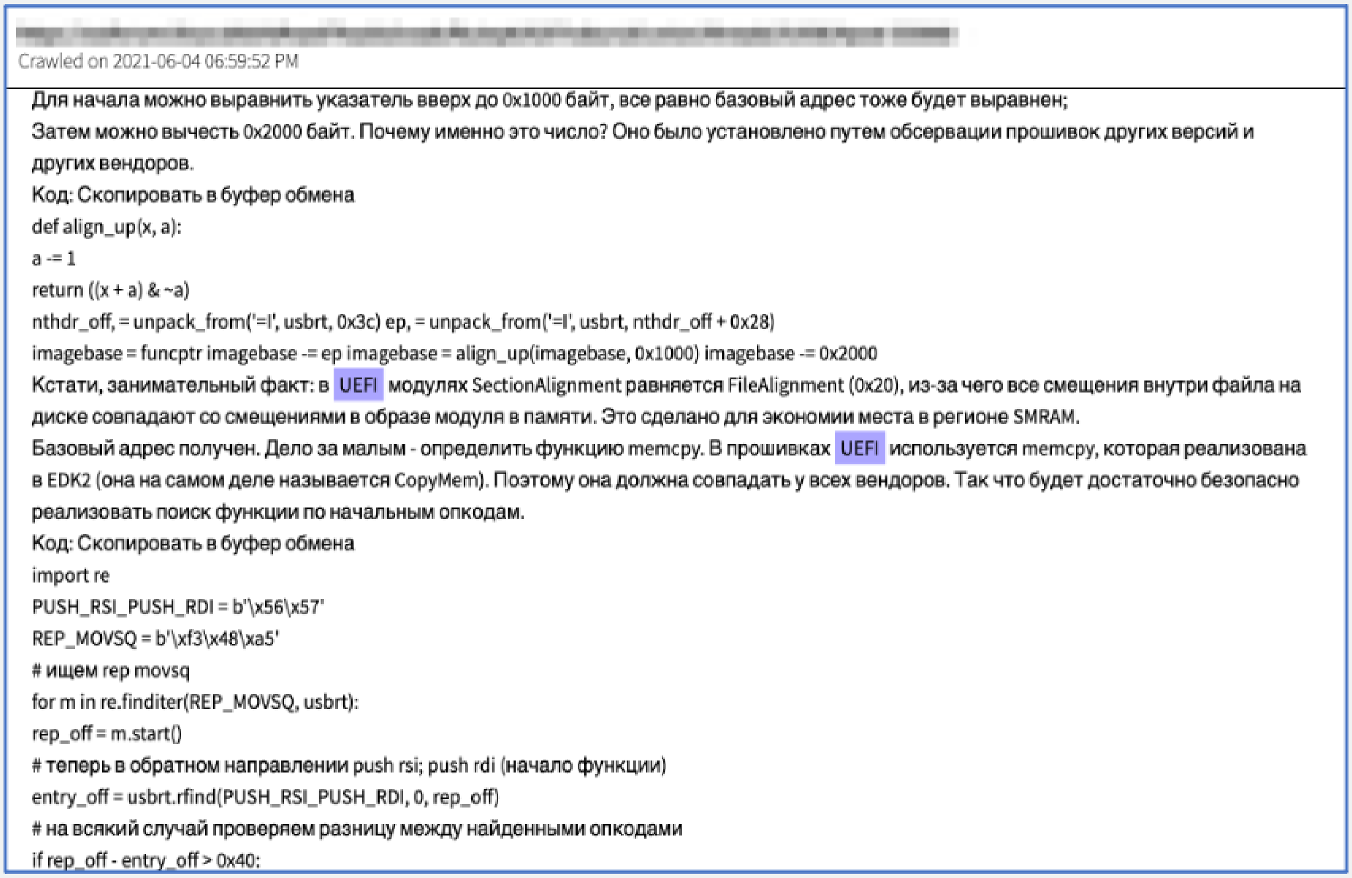
Given the how intertwined Trickbot and ransomware were last year, this threat vector, dubbed "Trickboot" intimates that it's only a matter of time - if it has not happened already - that ransomware affiliated malware had been embedded much deeper into victim networks for revisits and engagement by the threat actor long after the supposed incident was remediated or ransom payment and decryption occurred.

"TrickBot uses the RwDrv.sys driver from the open source, signed RWEverything project in order to interact with the SPI controller to see if the BIOS control register is unlocked such that the contents of the BIOS region can be modified," Scott added.

And yet, Trickboot is not the first instance of a UEFI exploit in the wild. Last fall, Kapersky issued a threat report detailing how they had discovered several compromised UEFI firmware images that had been modified by a malicious threat actor to drop malware onto associated victim devices. They had no indication of the infection mechanism, i.e. how the malicious module ended up in the firmware, but presented the threat as a "persistent installation" – likely to conduct extensive cyber espionage - on the infected laptop with telemetry indicating infections occurred as early as 2017. Digital fingerprints buried deep in the modules, such as samples of CurlReg code obtained by researchers linked what is now referred to as MosaicRegressor to Chinese state-sponsored threat actors.

In May 2021, a user on a popular hacking darknet forum detailed their experiments conducting BIOS/UEFI attacks (in Russian) on a Dell Inspiron 7567 laptop and how this could easily been exploited, posting: " ноутбук какого-нибудь члена Национального комитета Демократической партии США " [translated] "the laptop of some member of the National Committee of the Democratic Party of the United States," further solidifying the gravity of the forum post's contents.

[1] https://www.bleepingcomputer.com/news/security/intel-fixes-73-vulnerabilities-in-june-2021-platform-update/
[2] https://www.intel.com/content/www/us/en/security-center/default.html



[redacted]
Crawled on 2021-06-04 06:59:52 PM

Для начала можно выравнить указатель вверх до 0x1000 байт, все равно базовый адрес тоже будет выравнен;
Затем можно вычесть 0x2000 байт. Почему именно это число? Оно было установлено путем обсервации прошивок других версий и других вендоров.
Код: Скопировать в буфер обмена

```
def align_up(x, a):
a -= 1
return ((x + a) & ~a)
nthdr_off, = unpack_from('=I', usbrt, 0x3c) ep, = unpack_from('=I', usbrt, nthdr_off + 0x28)
imagebase = funcptr imagebase -= ep imagebase = align_up(imagebase, 0x1000) imagebase -= 0x2000
```

Кстати, занимательный факт: в UEFI модулях SectionAlignment равняется FileAlignment (0x20), из-за чего все смещения внутри файла на диске совпадают со смещениями в образе модуля в памяти. Это сделано для экономии места в регионе SMRAM.
Базовый адрес получен. Дело за малым - определить функцию memcpy. В прошивках UEFI используется memcpy, которая реализована в EDK2 (она на самом деле называется CopyMem). Поэтому она должна совпадать у всех вендоров. Так что будет достаточно безопасно реализовать поиск функции по начальным опкодам.
Код: Скопировать в буфер обмена

```
import re
PUSH_RSI_PUSH_RDI = b'\x56\x57'
REP_MOVSQ = b'\xf3\x48\xa5'
# ищем rep movsq
for m in re.finditer(REP_MOVSQ, usbrt):
rep_off = m.start()
# теперь в обратном направлении push rsi; push rdi (начало функции)
entry_off = usbrt.rfind(PUSH_RSI_PUSH_RDI, 0, rep_off)
# на всякий случай проверяем разницу между найденными опкодами
if rep_off - entry_off > 0x40:
```

Figure 4: Snippet From Lengthy Thread on Darknet Hacking Forum, Detailing how to Write BIOS/UEFI Malware to Intel Processors (Source: Screenshot from DarkOwl Vision)

By the end of the user's detailed instructions and code examples, they admit to having now developed a fully-automated exploit in their malware arsenal that allows them to not only execute code inside SMRAM (a.k.a. the system management memory of an Intel (x86) processor), but also arbitrarily read and write to any area of physical memory.

Security vulnerability researchers at Intel acknowledge the presence of an emerging BIOS/UEFI threat and less than a month ago released a major platform update that included over patches for 70 vulnerabilities across Intel's Virtualization Technology for Directed I/O (VT-d) products, Intel's Security Library and the BIOS firmware for Intel processors. Interestingly, over 40% of the security vulnerabilities involved graphics, networking, and Bluetooth components. [1,2]

In late June, Dell issued advisories affecting over 129 laptop hardware models after uncovering multiple vulnerabilities in HTTPS Boot and BIOSConnect that could expose the device to UEFI/BIOS exploits providing a malicious threat actor unauthorized elevated privilege to the OS and device firmware persistence. Dell recommended all customers update to the latest version of the Dell Client BIOS at their earliest opportunity to avoid possible infection. [3,4]

1. https://www.bleepingcomputer.com/news/security/intel-fixes-73-vulnerabilities-in-june-2021-platform-update/
2. https://www.intel.com/content/www/us/en/security-center/default.html
3. https://www.dell.com/support/kbdoc/en-us/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-biosconnect-feature-and-https-boot-feature
4. https://www.scmagazine.com/home/security-news/vulnerabilities/new-bios-vulnerabilities-impact-tens-of-millions-of-dell-computer-hardware/

CONCLUSIONS

It is clear the ransomware-as-a-service criminal industry is not going away anytime soon. Based on our observations and supporting evidence from industry experts, we can only expect that RaaS operators' TTPs will continue to become increasingly complex and the attacks more lethal in the future. It is especially important to consider the potential implications of the strong and deep network footholds that RaaS operators have established across multiple (and varied) industry sectors around the globe. Exposed credentials are still a viable threat attack vector along with use of "red team" commercial off-the-shelf network penetration toolsets and exploiting unpatched end-point security vulnerabilities in RDP/VPN protocols.

Launching the ransomware executable and encrypting critical files may be the end game for a RaaS attack; however, the activities of the threat actors while in the network and their persistent access and tools they leverage to give them the ability to revisit the victim's network (post-attack) should be more closely monitored and elevated as a subject of active discussions across the information security community.