SOPHOS
Cybersecurity delivered.

Multiple attackers: A clear and present danger

Competition has always been fierce among cryptominers and RATs, but ransomware bucks the trend.

Since their inception, the Sophos Managed Detection and Response (MDR) and Rapid Response (RR) teams have been called in to investigate hundreds of ransomware incidents, including intervening in active attacks where the attackers were still on the target's network.

In recent months, we've noticed an uptick in the number of cases where organizations have been attacked multiple times. Some attacks take place simultaneously; others are separated by a few days, weeks, or months. Some involve different kinds of malware, or double – even triple – infections of the same type.

Multiple attacks can be devastating for victims. Not only do they complicate remediation and business continuity plans, but the financial, reputational, and psychological impacts can be overwhelming. Our findings suggest a typical gap of around six weeks between attacks in cases where the same organization is attacked multiple times.

We wanted to explore how (and why) multiple attacks happen to certain targets. Recent case studies from our MDR and RR teams help illustrate the question of **how** these attacks transpire; cooperation and competition among threat actors can explain the **why**. Based on this analysis, we've provided eight pieces of advice that can help prevent multiple attacks.

By **Matt Wixey**, Sophos X-Ops

A Sophos X-Ops Active Adversary Whitepaper August 2022

Contents

Introduction

There's a well-worn industry phrase about the probability of a cyberattack: "It's not if, but when." But some of the incidents our Managed Detection and Response (MDR) and Rapid Response (RR) teams have investigated recently may force the industry to consider a change to this rule-of-thumb: The question is not if, or when – but how many times?

We've noticed an uptick in the number of cases where organizations have been attacked multiple times.[1] Some attacks take place simultaneously; others are separated by a few days, weeks, or months. Some involve different kinds of malware, or double – even triple – infections of the same type.

There are a variety of underlying causes, from big vulnerabilities and misconfigurations to threat actors competing for resources and dominance in an increasingly crowded threat environment.

Whatever the root cause, multiple attacks can be devastating for victims. Not only do they complicate remediation and business continuity plans, but the financial, reputational, and psychological impacts can be overwhelming. Just when you think that the worst has finally happened – and you now know for certain that it's 'when,' and not 'if' – you're hit with another attack. Our findings suggest a typical gap of around six weeks between attacks in cases where the same organization is attacked multiple times.

We wanted to explore how (and why) multiple attacks happen to certain targets. Recent case studies from our MDR and RR teams help illustrate the question of how these attacks transpire; cooperation and competition among threat actors can explain the why. Based on this analysis, we'll provide eight pieces of advice that can help prevent multiple attacks.

A sequence of unfortunate events

Unsurprisingly, the root causes of most multiple exploitations frequently come down to two issues: The targets fail to address significant exploitable vulnerabilities in either software or hardware; and, after an attack, victims fail to address malicious tooling or misconfigurations of hardware or software, left in place by the earlier attackers.

But there's a little more complexity to it than that. The cases we discuss below indicate that there's often a specific sequence of exploitation – cryptominers (a proverbial canary in the coal mine) arrive first, followed by wormable botnet builders (such as Mirai), then malware delivery systems (webshells and/or RATs), who may feed data to initial access brokers (IABs), and finally, ransomware.

Some of these threat actors are interdependent (IABs, for example, enable some ransomware attacks). Others will happily co-exist: Cryptominers and ransomware have different objectives, so they don't have any reason to directly interfere with each other[2] (although ransomware may encrypt cryptominers' configuration files, or artefacts from other attacks, like webshells – rendering those attacks inert).

We've also seen organizations hit by multiple ransomware attacks, sometimes because the threat actors didn't know a previous infection had occurred, but more often because they simply didn't care. One of the case studies we'll explore involved a *triple* ransomware incident, with some files being encrypted by three different ransomware strains. In that case, our investigation was complicated by the third threat actor not only erasing traces of their attack, but also those of the previous two.

On the other side of the coin, some threat actors don't play nicely together, and actively work against other infections or threat actors. Cryptominers, for example, often try to terminate the processes of other cryptominers, because CPU resources are finite, and a concurrent infection generates less revenue. There are exceptions, of course; some cryptominers, such as Outlaw, focus on different targets (IoT devices and Linux servers, via brute-force SSH attacks) to most of their rivals, and therefore aren't too concerned about competition. They may still have 'kill scripts' but rarely need to use them.[3]

We'll talk more about the relationships between threat actors shortly, but before that, let's look at a few examples of how big vulnerabilities can lead to multiple attacks.

The big bugs

The ProxyLogon (CVE-2021-26855[4]) and ProxyShell (CVE-2021-34473,[5] CVE-2021-34523,[6] and CVE-2021-31207[7]) vulnerabilities were first disclosed in March and August 2021, respectively. We covered both ProxyLogon and ProxyShell extensively at the time[8,9] and our follow-up research revealed that cryptominers – including Lemon Duck[10] and Tor2Mine[11] – were quick to take advantage. Tor2Mine even has a dedicated, heavily obfuscated 116-line PowerShell script designed to kill processes relating to over 70 competitors, including other miners, RATs, and 'clipper' malware that swaps cryptocurrency wallet addresses on a user's clipboard. The Squirrelwaffle malware delivery botnet also abused ProxyShell in 2021.[12]

Then came the ransomware. The earliest variants abusing ProxyLogon and ProxyShell appeared to be relatively crude, possibly because they were developed to exploit vulnerable hosts before they could be patched. These early variants included DearCry[13] and Black Kingdom ransomware,[14] which targeted organizations in March 2021.

Another new ransomware strain, LockFile,[15] was discovered in August, followed by Conti affiliate attacks in September 2021. In February 2022, we observed Conti attacking a healthcare organization at the same time as a Karma ransomware affiliate[16] (more on this one later, as we saw an interesting dynamic between the two groups in that case).

It's worth noting that attackers who exploit ProxyLogon/ProxyShell often drop webshells on compromised servers. If organizations were compromised, but didn't perform a clean-up after patching, there may still be many of these backdoors – and attacker-created email accounts – on now-patched Exchange servers, waiting for threat actors to use or sell them.

Log4Shell (CVE-2021-44228[17]), disclosed in December 2021, followed a similar sequence of events. In the days following the release of public proofs-of-concept, we observed a significant amount of scanning activity,[18] although not as many attacks as we expected. The lull didn't last; cryptominers soon arrived[19] (followed closely by webshells and backdoors deployed by IABs), and, as noted above, many came armed with functions for killing other miners.

Interestingly, Jin, a cryptominer we investigated in the above linked report, even terminated the Tomcat service vulnerable to Log4Shell, presumably to prevent other attackers from exploiting that infection vector. Threat actors locking the door after themselves isn't all that common, but it does happen, and we'll explore it later.

Exploitation of the recent remote code execution vulnerability in Atlassian[20] (CVE-2022-26134[21]) has, so far, followed the same pattern. As we previously reported, we saw attackers who exploited the Atlassian vulnerability deliver a variety of payloads, including cryptominers and webshells, followed some time later by ransomware attempts.

Takeaway 1: Updates for absolutely everything

It sounds simple, but: Update everything. One of our key findings is that cryptominers, and webshells and backdoors deployed by IABs, often come first when a vulnerability has been disclosed, and the latter typically try to operate stealthily – so you might think you've avoided an attack, when in fact there's already malware on your system. That might be compounded (in a subsequent attack) by ransomware. Patching early is the best way to avoid being compromised in the future – but it doesn't mean you haven't already been attacked. It's always worth checking that your organization wasn't breached prior to patching.

Takeaway 2: Prioritize the worst bugs first

But how can you patch early, and how do you know what to patch? Prioritizing can be a big ask, given how many vulnerabilities are disclosed (18,429 in 2021,[22] more than 50 a day on average, and the greatest number of reported vulnerabilities ever disclosed during a calendar year). So focus on two key elements: 1) critical bugs affecting your specific software stack; and 2) high-profile vulnerabilities that could affect your technology. There are paid services which offer vulnerability intelligence, but there are also free tools which let you set up custom alerts for particular products. Bug Alert[23] is a non-profit service that aims to give early warning of high impact bugs. Monitoring 'infosec Twitter' is also recommended, as that's where many prominent vulnerabilities are discussed when first released. Or you could use CVE Trends,[24] which collates data from several sites to show the most-talked-about vulnerabilities.

Leaving the door open

Remote access misconfigurations – typically internet-exposed, unsecured RDP servers, as well as applications like RDWeb or AnyDesk – are also a leading cause of multiple attacks, when incident responders fail to address the misconfiguration after the first incident. In the following case study, the first threat actor used RDP to gain access. But the issue wasn't fixed, leading to a second attack.

Case study: Exposed RDP applications lead to two attacks in five weeks

April 8th 2022: A threat actor gains access to an organization's network via an unsecured RDP server.

April 12th: The threat actor installs Advanced IP Scanner[25] to gather information about other devices on the network.

April 13th: The threat actor makes further RDP connections, adds a new administrative user, and executes Mimikatz.[26]

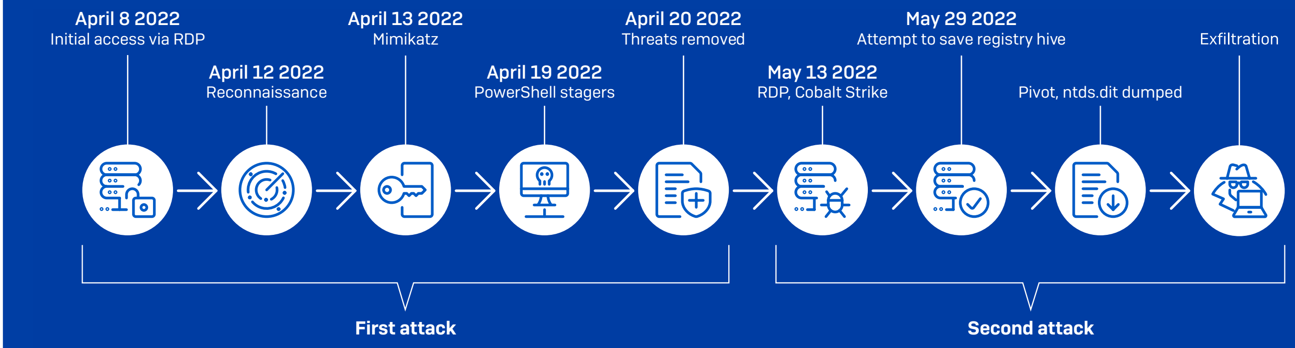
April 19th: The attacker downloads several PowerShell malware stagers associated with keylogging and remote command execution.

April 20th: The organization removes the threats. Sophos' MDR team makes several recommendations, including disabling RDP access from the internet for several hosts, resetting passwords for compromised users, and performing a domain-wide credential reset. Some of these recommendations are not followed.

May 13th: A second threat actor authenticates over RDP to one of the hosts which Sophos recommended be secured after the previous attack. Cobalt Strike[27] activity is observed.

May 27th: The threat actor authenticates over RDP.

May 29th: The threat actor performs reconnaissance on the domain, changes the credentials for an account, and attempts to save the registry hive. When this fails, they continue to perform reconnaissance, pivot to another host, and dump the **ntds.dit** file, a database of Active Directory information, including password hashes for all domain users. DNS requests for **anonfiles[.]com** and **fex[.]net**, file-sharing services popular with threat actors, are observed. The threat actor manages to upload a small amount of data, before the attack is stopped a few minutes later.



Sophos X-Ops

Figure 1: Timeline of the attack

Takeaway 3: Mind your configurations

Misconfigurations – and a failure to remediate them after an attack – are a leading cause of multiple exploitations. Cryptominer operators, IABs, and ransomware affiliates always look for exposed RDP and VPN ports, and they're among the most popular listings on most criminal marketplaces. If you do need remote access and/or management over the internet, put it behind a VPN or a zero-trust network access solution that uses MFA as part of its login procedure.

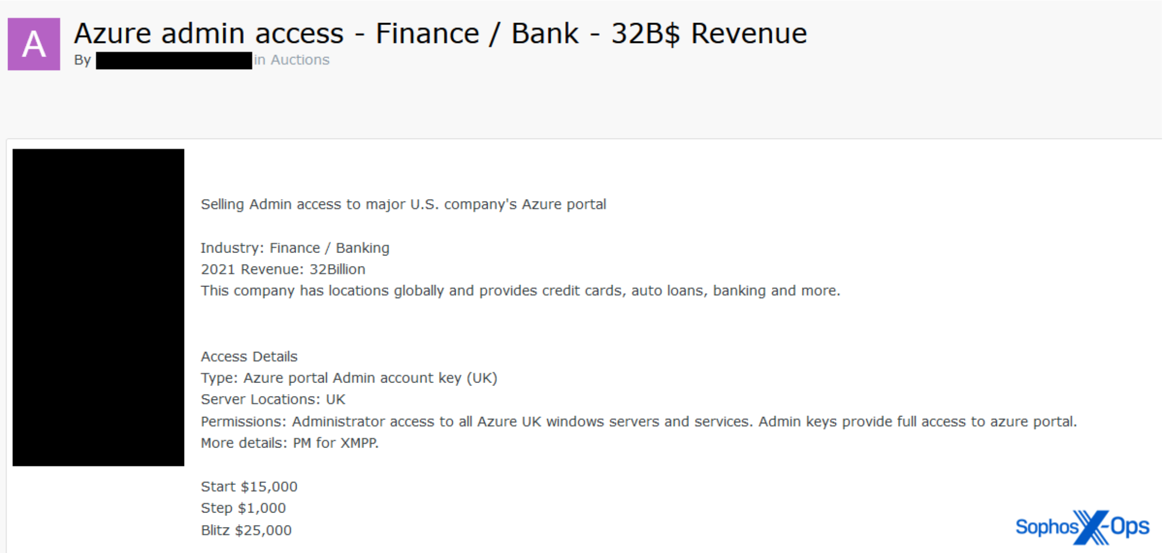
Selling access to your network to the highest bidder

Prominent vulnerabilities and misconfigurations can lead to compromises. It shouldn't come as a surprise that, if the underlying issues aren't addressed after an attack, another threat actor might find and exploit them too. In fact, it's quite likely, given the amount of scanning that threat actors do.

But there can be many other causes of multiple attacks. Earlier we briefly discussed the differing priorities of cryptominers and ransomware, so let's take a closer look at how some features of the criminal ecosystem might contribute to multiple attacks.

Criminals buy access to networks from IABs on criminal marketplaces (this is sometimes referred to as Access-as-a-Service, or AaaS[28]). Because IABs don't want the victim to be alerted that a compromise has occurred, they usually omit organization names and identifying information from their listings, but will include details about sector, revenue, the size of the network, and what type of access is being offered, to attract potential buyers. In some cases, AaaS listings are auctioned off to the highest bidder. In others, it's down to interested parties to approach the seller privately and negotiate (usually away from the forum, on chat platforms like Jabber and Tox).

Here's a typical AaaS listing on a prominent Russian-language criminal forum:



A Azure admin access - Finance / Bank - 32B$ Revenue

By [redacted] in Auctions

[redacted]

Selling Admin access to major U.S. company's Azure portal

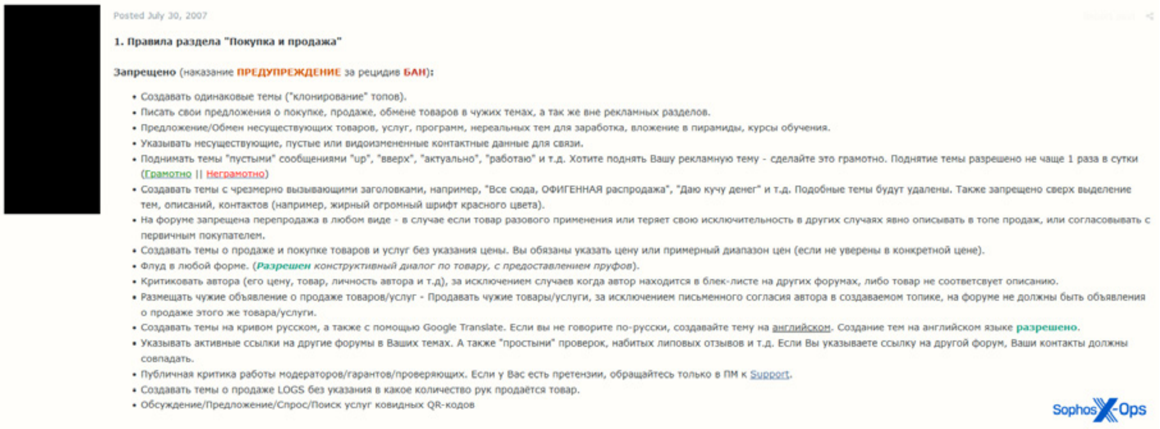
Industry: Finance / Banking
2021 Revenue: 32Billion
This company has locations globally and provides credit cards, auto loans, banking and more.

Access Details
Type: Azure portal Admin account key (UK)
Server Locations: UK
Permissions: Administrator access to all Azure UK windows servers and services. Admin keys provide full access to azure portal.
More details: PM for XMPP.

Start $15,000
Step $1,000
Blitz $25,000

Figure 2: An AaaS listing on a criminal marketplace. This listing is being offered for auction, with start, step, and blitz (instant sale) prices provided

Notice anything? There's no mention of exclusivity. And if we look at this forum's rules, we see something interesting. Roughly translated, one of the rules includes this instruction: "If the product is a one-time use or loses its exclusivity in other cases, clearly say so at the top of the listing, or coordinate with the primary buyer."



[redacted]

Posted July 30, 2007

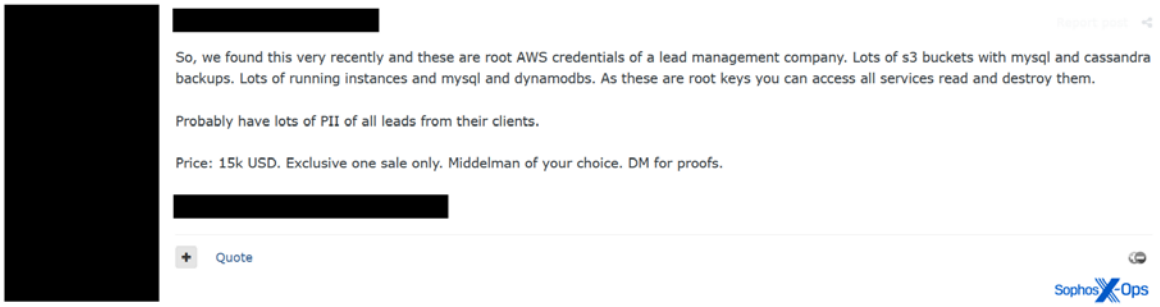
1. Правила раздела "Покупка и продажа"

Запрещено (наказание **ПРЕДУПРЕЖДЕНИЕ** за рецидив **БАН**):

- Создавать одинаковые темы ("клонирование" топов).
- Писать свои предложения о покупке, продаже, обмене товаров в чужих темах, а так же вне рекламных разделов.
- Предложение/Обмен несуществующих товаров, услуг, программ, нереальных тем для заработка, вложение в пирамиды, курсы обучения.
- Указывать несуществующие, пустые или видоизмененные контактные данные для связи.
- Поднимать темы "пустыми" сообщениями "up", "вверх", "актуально", "работаю" и т.д. Хотите поднять Вашу рекламную тему - сделайте это грамотно. Поднятие темы разрешено не чаще 1 раза в сутки (Грамотно || Неграмотно)
- Создавать темы с чрезмерно вызывающими заголовками, например, "Все сюда, ОФИГЕННАЯ распродажа", "Даю кучу денег" и т.д. Подобные темы будут удалены. Также запрещено сверх выделение тем, описаний, контактов (например, жирный огромный шрифт красного цвета).
- На форуме запрещена перепродажа в любом виде - в случае если товар разового применения или теряет свою исключительность в других случаях явно описывать в топе продаж, или согласовывать с первичным покупателем.
- Создавать темы о продаже и покупке товаров и услуг без указания цены. Вы обязаны указать цену или примерный диапазон цен (если не уверены в конкретной цене).
- Флуд в любой форме. (***Разрешен*** *конструктивный диалог по товару, с предоставлением пруфов*).
- Критиковать автора (его цену, товар, личность автора и т.д), за исключением случаев когда автор находится в блек-листе на других форумах, либо товар не соответсвует описанию.
- Размещать чужие объявление о продаже товаров/услуг - Продавать чужие товары/услуги, за исключением письменного согласия автора в создаваемом топике, на форуме не должны быть объявления о продаже этого же товара/услуги.
- Создавать темы на кривом русском, а также с помощью Google Translate. Если вы не говорите по-русски, создавайте тему на английском. Создание тем на английском языке **разрешено**.
- Указывать активные ссылки на другие форумы в Ваших темах. А также "простыни" проверок, набитых липовых отзывов и т.д. Если Вы указываете ссылку на другой форум, Ваши контакты должны совпадать.
- Публичная критика работы модераторов/гарантов/проверяющих. Если у Вас есть претензии, обращайтесь только в ПМ к Support.
- Создавать темы о продаже LOGS без указания в какое количество рук продаётся товар.
- Обсуждение/Предложение/Спрос/Поиск услуг ковидных QR-кодов

Figure 3: The forum rules for buying and selling

In other words, sellers are supposed to give a clear indication as to whether a listing is exclusive. Here's an example of a listing that explicitly promises exclusivity, stating "Exclusive one sale only":



[redacted]

[redacted]

So, we found this very recently and these are root AWS credentials of a lead management company. Lots of s3 buckets with mysql and cassandra backups. Lots of running instances and mysql and dynamodbs. As these are root keys you can access all services read and destroy them.

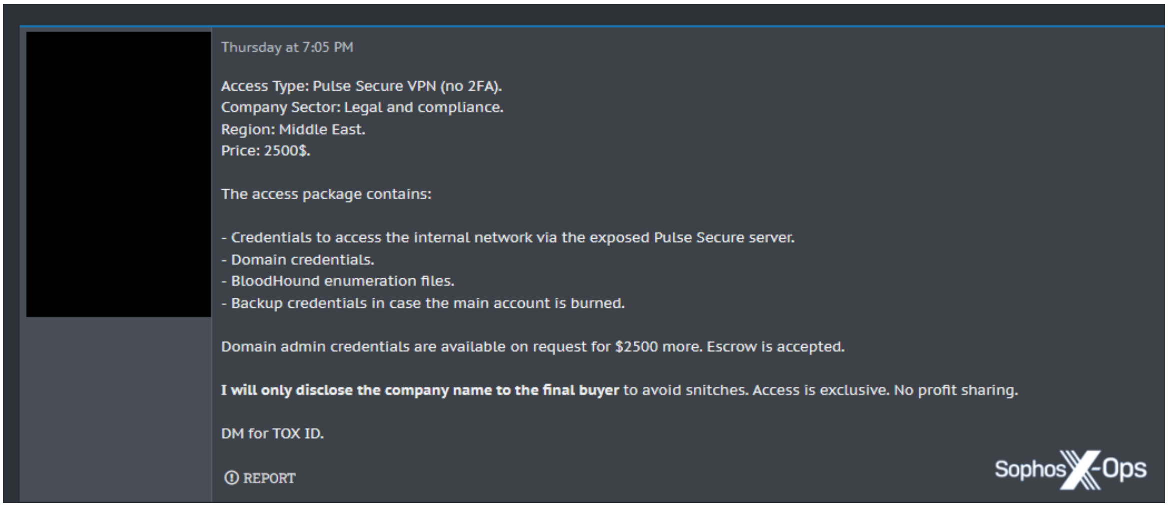
Probably have lots of PII of all leads from their clients.

Price: 15k USD. Exclusive one sale only. Middelman of your choice. DM for proofs.

[redacted]

Figure 4: An exclusive listing on a criminal marketplace

This isn't specific to this forum, either – here's an example from another prominent criminal site, where the seller writes: "**I will only disclose the company name to the final buyer** to avoid snitches. Access is exclusive. No profit sharing." [emphasis in original]



[redacted]

Thursday at 7:05 PM

Access Type: Pulse Secure VPN (no 2FA).
Company Sector: Legal and compliance.
Region: Middle East.
Price: 2500$.

The access package contains:

- Credentials to access the internal network via the exposed Pulse Secure server.
- Domain credentials.
- BloodHound enumeration files.
- Backup credentials in case the main account is burned.

Domain admin credentials are available on request for $2500 more. Escrow is accepted.

I will only disclose the company name to the final buyer to avoid snitches. Access is exclusive. No profit sharing.

DM for TOX ID.

Figure 5: An exclusive listing on a second criminal marketplace, this one for VPN access to an organization in the Middle East

But these tend to be the exception; many listings don't include any mention of exclusivity at all. And while reselling is generally forbidden on forums, it's entirely possible that many AaaS listings are non-exclusive, and sold to multiple buyers to take advantage of growing demand – resulting in multiple attacks. In fact, on some marketplaces, such as Genesis, exclusivity can even require an additional fee.

As an interesting side note, it appears that ransomware affiliate membership isn't always exclusive either; some threat actors are members of multiple programs. For example, we recently investigated cases where Hive and Conti ransomware variants shared the same infrastructure, despite the two groups having notable differences in their strategies, communication styles, and levels of operational security.[29]

Case study: Ransomware affiliate uses both Hive and Conti

In March 2022, Sophos' MDR team responds to a Conti ransomware incident, where the threat actor abused MSBuild.exe[30] to execute **Cobalt Strike**, beaconing to **edgecloud[.]ink**.

A few days later, the MDR team responds to a separate incident involving Hive ransomware, where the threat actor once again abused **MSBuild.exe** to execute **Cobalt Strike**, and beaconed to the same domain.

The MDR team has since responded to other Hive ransomware incidents with overlapping infrastructure – suggesting this activity is likely from a single ransomware affiliate.

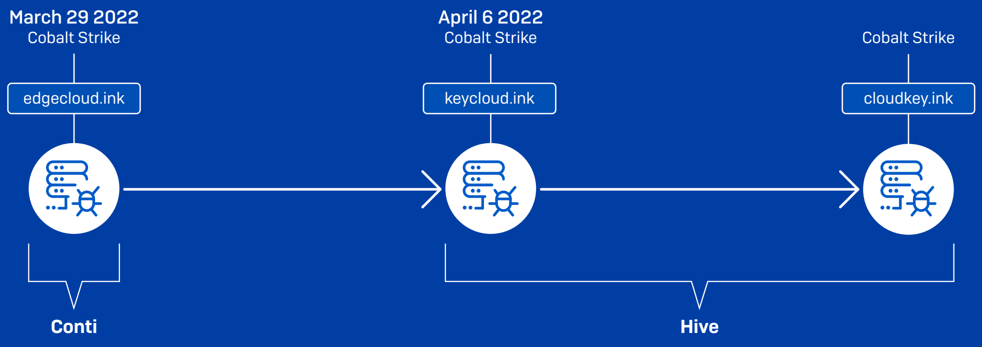
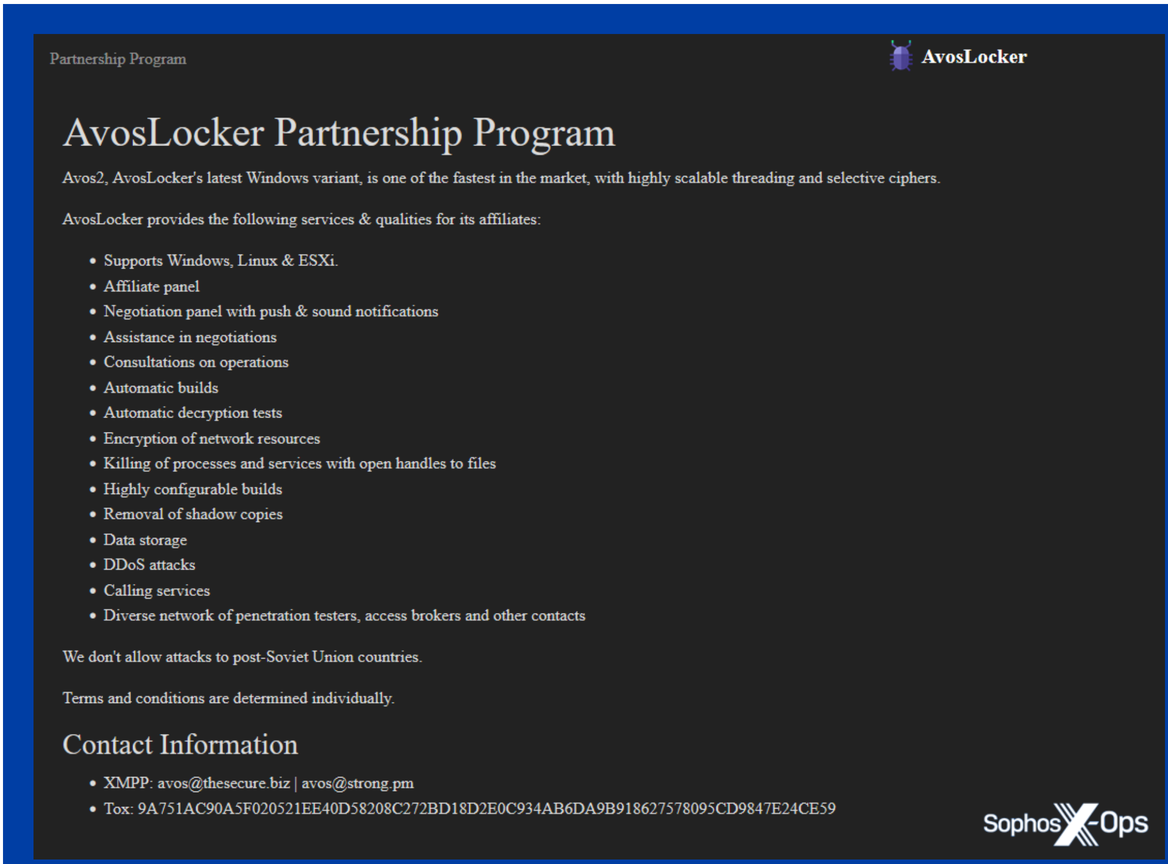


Figure 6: Shared infrastructure observed in recent Hive and Conti ransomware attacks in March and April 2022



Partnership Program

AvosLocker

AvosLocker Partnership Program

Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

AvosLocker provides the following services & qualities for its affiliates:

- Supports Windows, Linux & ESXi.
- Affiliate panel
- Negotiation panel with push & sound notifications
- Assistance in negotiations
- Consultations on operations
- Automatic builds
- Automatic decryption tests
- Encryption of network resources
- Killing of processes and services with open handles to files
- Highly configurable builds
- Removal of shadow copies
- Data storage
- DDoS attacks
- Calling services
- Diverse network of penetration testers, access brokers and other contacts

We don't allow attacks to post-Soviet Union countries.

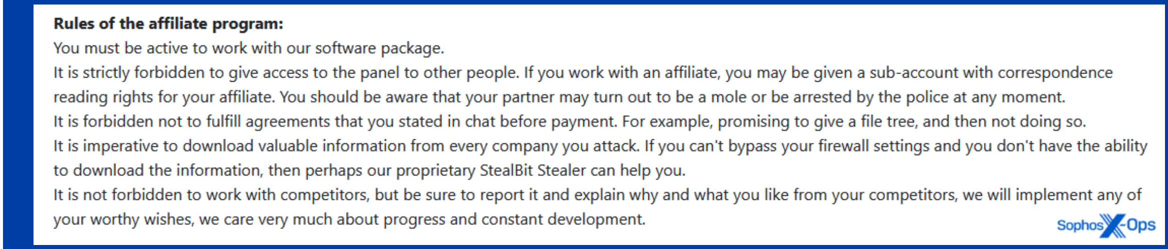
Terms and conditions are determined individually.

Contact Information

- XMPP: avos@thesecure.biz | avos@strong.pm
- Tox: 9A751AC90A5F020521EE40D58208C272BD18D2E0C934AB6DA9B918627578095CD9847E24CE59

Figure 7: Details of the AvosLocker affiliate scheme

Lockbit's affiliate rules, on the other hand, explicitly state that working with competitors is "not forbidden…but be sure to report it and explain why and what you like from your competitors":



Rules of the affiliate program:
You must be active to work with our software package.
It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.
It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.
It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.
It is not forbidden to work with competitors, but be sure to report it and explain why and what you like from your competitors, we will implement any of your worthy wishes, we care very much about progress and constant development.

Figure 8: Details of the Lockbit affiliate scheme, referring to working with competitors

And as we'll see in our next case studies, ransomware threat actors sometimes benefit from each other's activities, and don't seem to be overly concerned about competition

Another possible reason for multiple attacks may be the existence of leak sites. Ransomware gangs publish information about their victims, sometimes along with stolen data (the new Lockbit 3.0 site even lets others bid to immediately access – or destroy – the data, putting more pressure on the victim to pay the ransom).

As security researcher Kevin Beaumont has pointed out,[31] contrary to popular opinion, targets who haven't responded to the ransom demands comprise most of the victims whose details have been disclosed on leak sites.

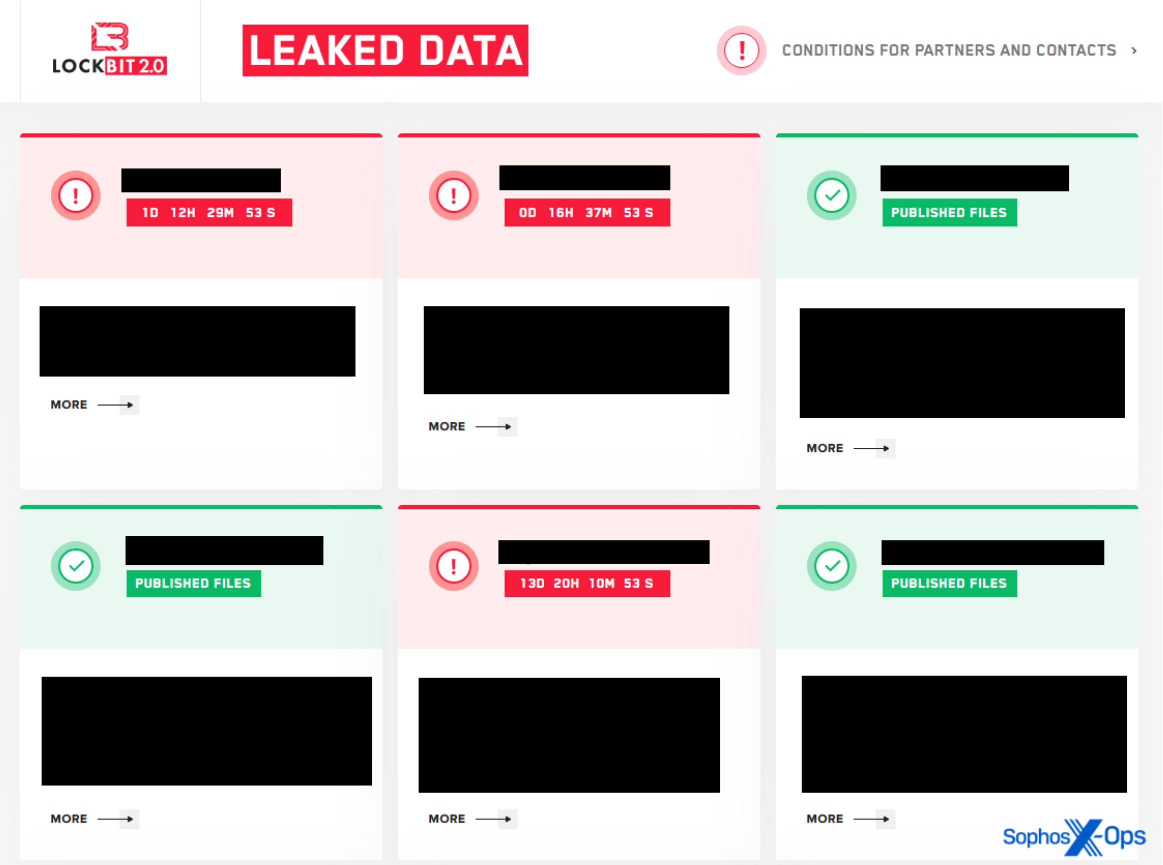
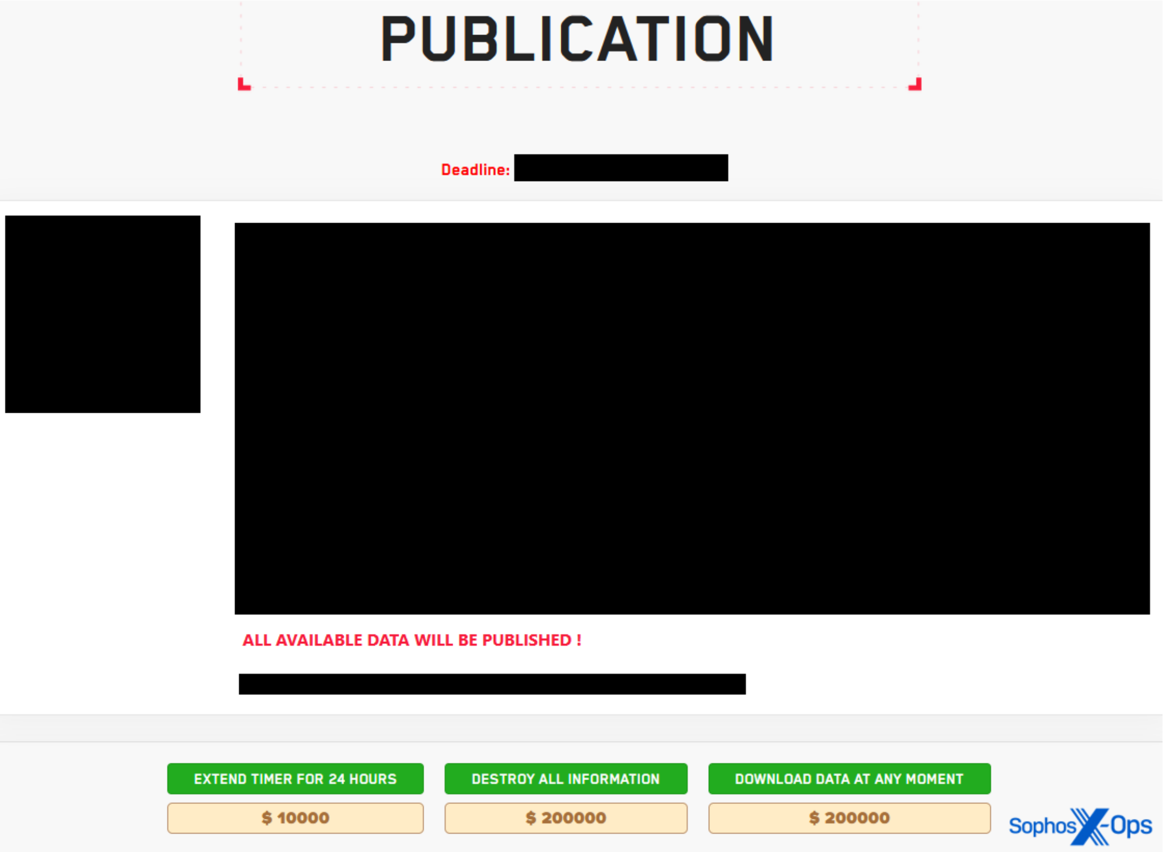


Figure 9: The Lockbit 2.0 leak site, showing details of current and past victims (redacted)



PUBLICATION

Deadline: [redacted]

[redacted]

[redacted]

ALL AVAILABLE DATA WILL BE PUBLISHED !

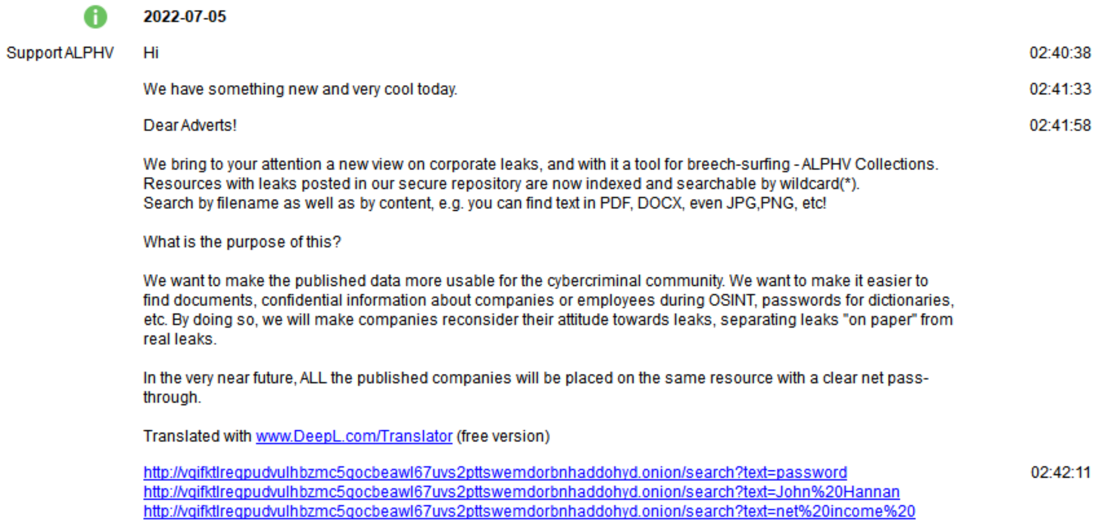
[redacted]

Figure 10: The Lockbit 3.0 leak site, complete with a public auction enabling anyone to pay to extend the timer, or destroy or download the organization's data. A gallery of screenshots from the compromised network is provided as proof

Why might that result in multiple attacks? Leak sites are public. An opportunistic, lower-tier ransomware actor might reason that, if a victim hasn't responded to a ransom demand, they might not have addressed the infection vector, either. The threat actor has nothing to lose: Unlike buying an AaaS listing, it won't cost them anything to target organizations that appear on leak sites.

Besides, the first ransomware attack might have failed to encrypt everything; if the second threat actor encrypts further files, it may put additional pressure on the victim to pay up. We'll discuss whether multiple attacks benefit or disadvantage ransomware groups in the next section.

Non-ransomware threat actors might also seize on the data published on leak sites – including personal information and passwords – to enable further attacks. Some ransomware groups actively encourage this; ALPHV/BlackCat recently announced[32] that they have made their leaks searchable, "to make the published data more usable for the cybercriminal community."



2022-07-05

Support ALPHV Hi 02:40:38

We have something new and very cool today. 02:41:33

Dear Adverts! 02:41:58

We bring to your attention a new view on corporate leaks, and with it a tool for breech-surfing - ALPHV Collections.
Resources with leaks posted in our secure repository are now indexed and searchable by wildcard(*).
Search by filename as well as by content, e.g. you can find text in PDF, DOCX, even JPG,PNG, etc!

What is the purpose of this?

We want to make the published data more usable for the cybercriminal community. We want to make it easier to find documents, confidential information about companies or employees during OSINT, passwords for dictionaries, etc. By doing so, we will make companies reconsider their attitude towards leaks, separating leaks "on paper" from real leaks.

In the very near future, ALL the published companies will be placed on the same resource with a clear net pass-through.

Translated with www.DeepL.com/Translator (free version)

http://vgifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd.onion/search?text=password 02:42:11
http://vgifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd.onion/search?text=John%20Hannan
http://vgifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd.onion/search?text=net%20income%20

Figure 11: A message from the ALPHV/BlackCat ransomware group to its affiliates. (Image source: @vxunderground[33])

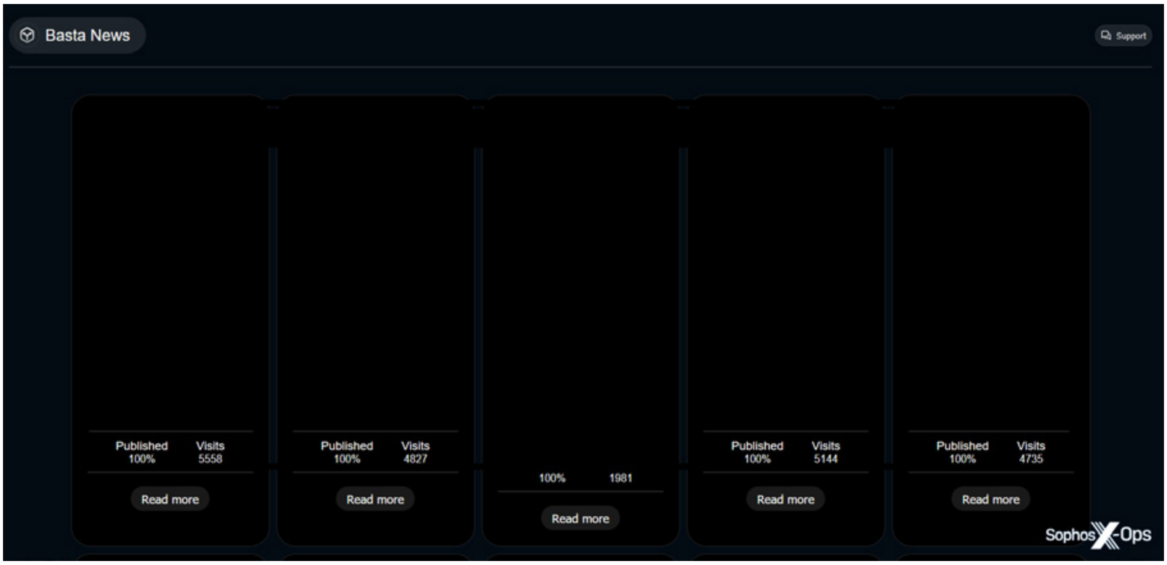


Figure 12: The Black Basta ransomware leak site (organization names redacted)

Takeaway 4: Assume other attackers have found your vulnerabilities

Threat actors don't operate in isolation. IABs might resell or relist their products, and ransomware affiliates may use multiple strains – so one vulnerability or misconfiguration can lead to multiple threat actors seeking to exploit your network.

Takeaway 5: Don't slow-walk addressing an attack in progress

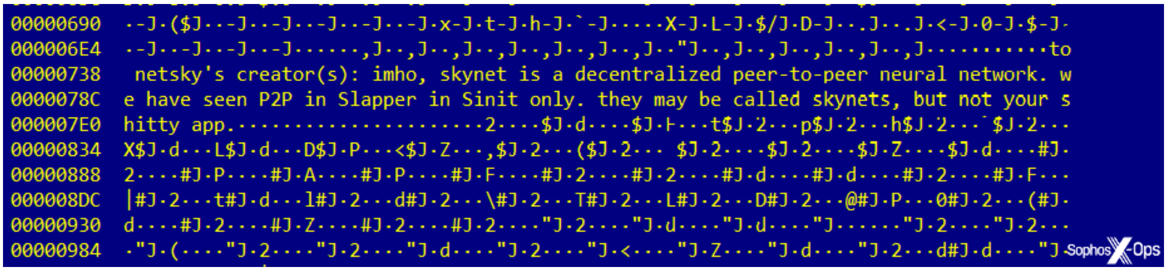
Being listed on a leak site may attract other, opportunistic threat actors. If you're unfortunate enough to be hit with a ransomware attack, take immediate action, in conjunction with your security teams and incident response provider(s), to close the initial entry point and assess what data has been leaked, as part of your wider remediation plan.

Why can’t we be friends?

So what do the threat actors think about all this? Do they like sharing space, is it a necessary evil, or will they kick each other off infected systems given half a chance?

The history of malware[34] tells us that, in the past, the concept of cooperation (or, at the very least, peaceful co-existence) seemed alien to many threat actors. Alliances were few, often fragile, and could turn to enmity at the smallest slight. Malware authors fought, constantly – over hosts, bragging rights, technical skills, and botnet numbers.

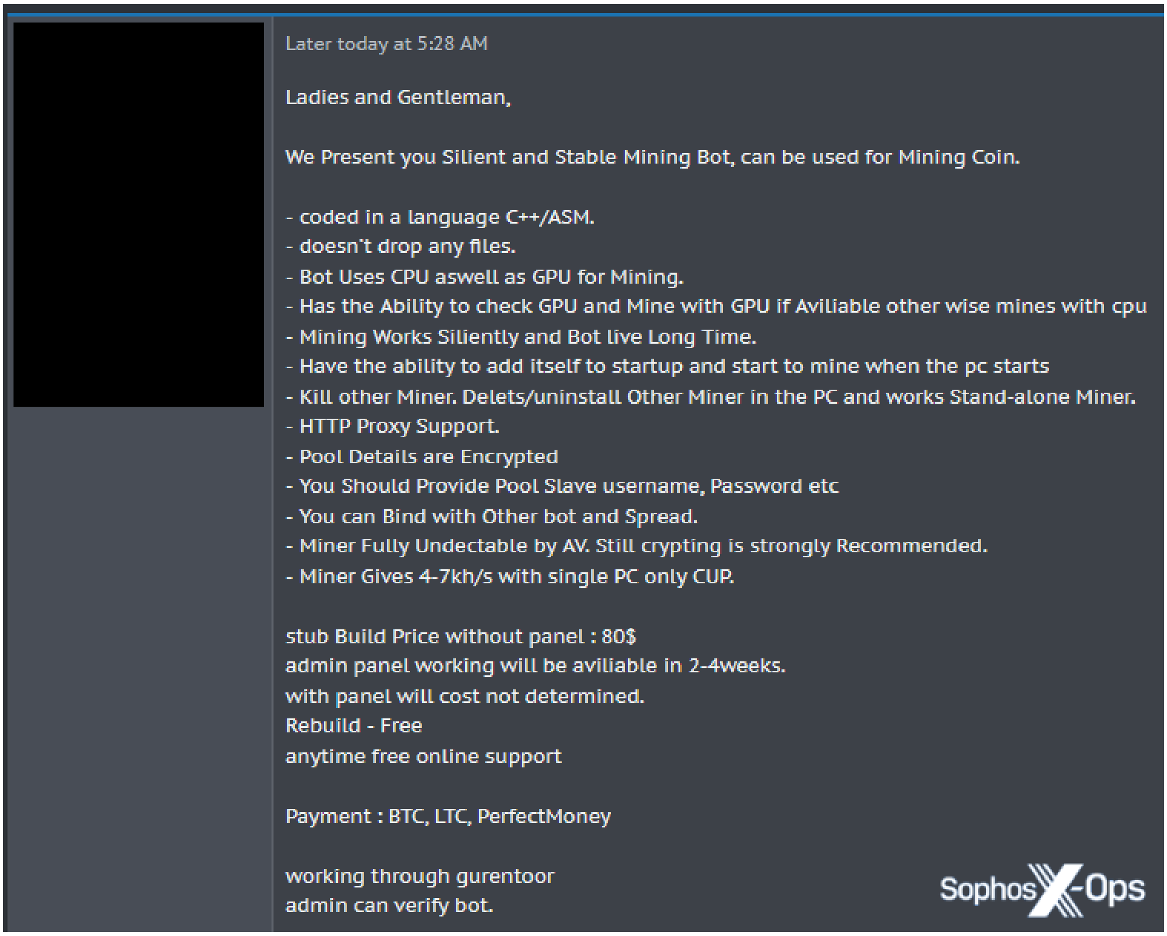
In the mid-2000s, at the height of the ‘worm wars’, it was common for worms to contain specific routines designed to remove other, competing worms, and to immunize themselves from attempts to be removed. These battles were just as cutthroat as those that take place between cryptominers today; the developers of Netsky, Bagle, and Mydoom even traded insults in their source code, leading Graham Cluley – a senior technology consultant at Sophos at the time – to comment: “I would much rather they ranted at each other on message boards instead of in raw code.”[35]



```
00000690  --J·($J---J---J---J---J---J·x-J·t-J·h-J·`-J·····X-J·L-J·$/J·D-J···J···J·<-J·0-J·$-J·
000006E4  --J---J---J---J······,J··,J··,J··,J··,J··,J··,J··"J··,J··,J··,J··,J··,J··········to
00000738   netsky's creator(s): imho, skynet is a decentralized peer-to-peer neural network. w
0000078C  e have seen P2P in Slapper in Sinit only. they may be called skynets, but not your s
000007E0  hitty app.······················2····$J·d····$J·⊦···t$J·2···p$J·2···h$J·2···`$J·2···
00000834  X$J·d···L$J·d···D$J·P···<$J·Z···,$J·2···($J·2··· $J·2····$J·2····$J·Z····$J·d····#J·
00000888  2····#J·P····#J·A····#J·P····#J·F····#J·2····#J·2····#J·d····#J·d····#J·2····#J·F···
000008DC  |#J·2···t#J·d···l#J·2···d#J·2···\#J·2···T#J·2···L#J·2···D#J·2···@#J·P···0#J·2···(#J·
00000930  d····#J·2····#J·Z····#J·2····#J·2····"J·2····"J·d····"J·d····"J······"J·2····"J·2···
00000984  ·"J·(····"J·2····"J·2····"J·d····"J·2····"J·<····"J·Z····"J·d····"J·2···d#J·d····"J
```

Figure 13: The Mydoom author exchanges pleasantries with the Netsky developer in March 2004

Much like worms, cryptominers often employ a botnet model, albeit for different reasons. Cryptomining is a low-yield, high-volume business model, so lots of infections are required for an acceptable return, and every infected host’s CPU resources have to be maximized. That’s why cryptominers have contained routines to kill rivals pretty much since their inception. We dug deep into the archives of one criminal forum and found a cryptominer specification sheet from 2014, offering “kill other Miner” [sic] as a feature for would-be buyers.



[redacted]

Later today at 5:28 AM

Ladies and Gentleman,

We Present you Silient and Stable Mining Bot, can be used for Mining Coin.

- coded in a language C++/ASM.
- doesn't drop any files.
- Bot Uses CPU aswell as GPU for Mining.
- Has the Ability to check GPU and Mine with GPU if Aviliable other wise mines with cpu
- Mining Works Siliently and Bot live Long Time.
- Have the ability to add itself to startup and start to mine when the pc starts
- Kill other Miner. Delets/uninstall Other Miner in the PC and works Stand-alone Miner.
- HTTP Proxy Support.
- Pool Details are Encrypted
- You Should Provide Pool Slave username, Password etc
- You can Bind with Other bot and Spread.
- Miner Fully Undectable by AV. Still crypting is strongly Recommended.
- Miner Gives 4-7kh/s with single PC only CUP.

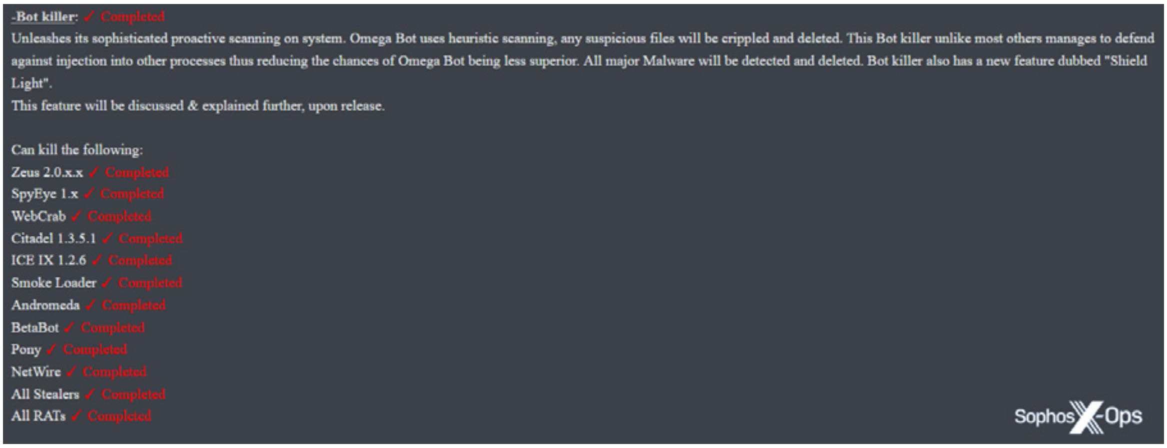
stub Build Price without panel : 80$
admin panel working will be aviliable in 2-4weeks.
with panel will cost not determined.
Rebuild - Free
anytime free online support

Payment : BTC, LTC, PerfectMoney

working through gurentoor
admin can verify bot.

Figure 14: An advert for a cryptominer, posted on a criminal forum in 2014

The hostilities aren't confined to worms and cryptominers, of course. Back in the early 2010s, the crimeware kit SpyEye[36] had a feature designed to hijack or remove infections[37] by one of its competitors, Zeus[38] (although the two may have later merged[39]). And in 2013, a malware package known as Omega Bot claimed it could remove not only Zeus and SpyEye, but a host of other competitors:

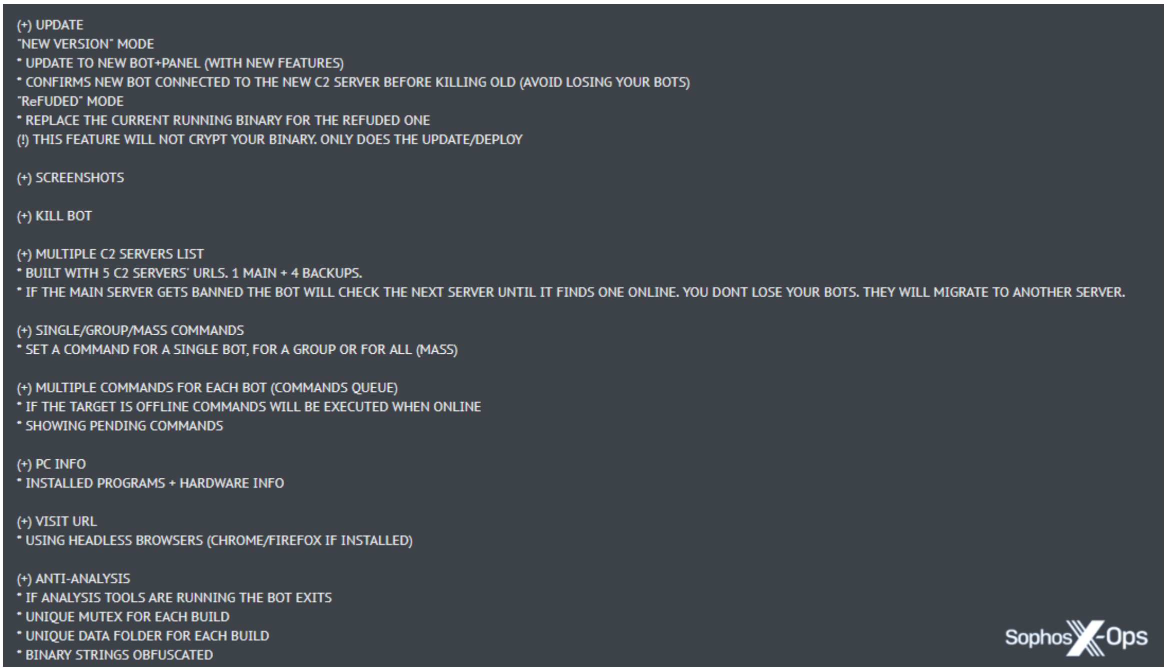


-Bot killer: ✓ Completed
Unleashes its sophisticated proactive scanning on system. Omega Bot uses heuristic scanning, any suspicious files will be crippled and deleted. This Bot killer unlike most others manages to defend against injection into other processes thus reducing the chances of Omega Bot being less superior. All major Malware will be detected and deleted. Bot killer also has a new feature dubbed "Shield Light".
This feature will be discussed & explained further, upon release.

Can kill the following:
Zeus 2.0.x.x ✓ Completed
SpyEye 1.x ✓ Completed
WebCrab ✓ Completed
Citadel 1.3.5.1 ✓ Completed
ICE IX 1.2.6 ✓ Completed
Smoke Loader ✓ Completed
Andromeda ✓ Completed
BetaBot ✓ Completed
Pony ✓ Completed
NetWire ✓ Completed
All Stealers ✓ Completed
All RATs ✓ Completed

Figure 15: Omega Bot offered for sale on a criminal forum in 2013

This has continued until the present day, with modern RATs highlighting **bot killing** as a feature. The spec sheet for Spectre RAT, offered for sale in June 2022, has this:



(+) UPDATE
"NEW VERSION" MODE
* UPDATE TO NEW BOT+PANEL (WITH NEW FEATURES)
* CONFIRMS NEW BOT CONNECTED TO THE NEW C2 SERVER BEFORE KILLING OLD (AVOID LOSING YOUR BOTS)
"ReFUDED" MODE
* REPLACE THE CURRENT RUNNING BINARY FOR THE REFUDED ONE
(!) THIS FEATURE WILL NOT CRYPT YOUR BINARY. ONLY DOES THE UPDATE/DEPLOY

(+) SCREENSHOTS

(+) KILL BOT

(+) MULTIPLE C2 SERVERS LIST
* BUILT WITH 5 C2 SERVERS' URLS. 1 MAIN + 4 BACKUPS.
* IF THE MAIN SERVER GETS BANNED THE BOT WILL CHECK THE NEXT SERVER UNTIL IT FINDS ONE ONLINE. YOU DONT LOSE YOUR BOTS. THEY WILL MIGRATE TO ANOTHER SERVER.

(+) SINGLE/GROUP/MASS COMMANDS
* SET A COMMAND FOR A SINGLE BOT, FOR A GROUP OR FOR ALL (MASS)

(+) MULTIPLE COMMANDS FOR EACH BOT (COMMANDS QUEUE)
* IF THE TARGET IS OFFLINE COMMANDS WILL BE EXECUTED WHEN ONLINE
* SHOWING PENDING COMMANDS

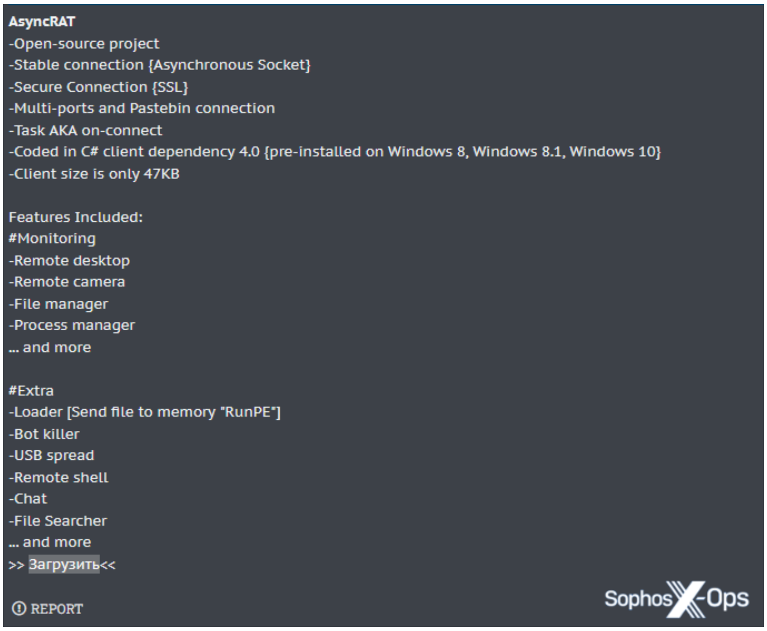
(+) PC INFO
* INSTALLED PROGRAMS + HARDWARE INFO

(+) VISIT URL
* USING HEADLESS BROWSERS (CHROME/FIREFOX IF INSTALLED)

(+) ANTI-ANALYSIS
* IF ANALYSIS TOOLS ARE RUNNING THE BOT EXITS
* UNIQUE MUTEX FOR EACH BUILD
* UNIQUE DATA FOLDER FOR EACH BUILD
* BINARY STRINGS OBFUSCATED

Figure 16: The latest version of the Spectre RAT, advertised on a criminal forum

And a version of AsyncRAT,[40] which researchers recently observed[41] exploiting the Follina vulnerability[42] (CVE-2022-30190[43]), offers "bot killer" as a bonus feature in this advert from December 2021:



AsyncRAT
-Open-source project
-Stable connection {Asynchronous Socket}
-Secure Connection {SSL}
-Multi-ports and Pastebin connection
-Task AKA on-connect
-Coded in C# client dependency 4.0 {pre-installed on Windows 8, Windows 8.1, Windows 10}
-Client size is only 47KB

Features Included:
#Monitoring
-Remote desktop
-Remote camera
-File manager
-Process manager
... and more

#Extra
-Loader [Send file to memory "RunPE"]
-Bot killer
-USB spread
-Remote shell
-Chat
-File Searcher
... and more
>> Загрузить<<

ⓘ REPORT

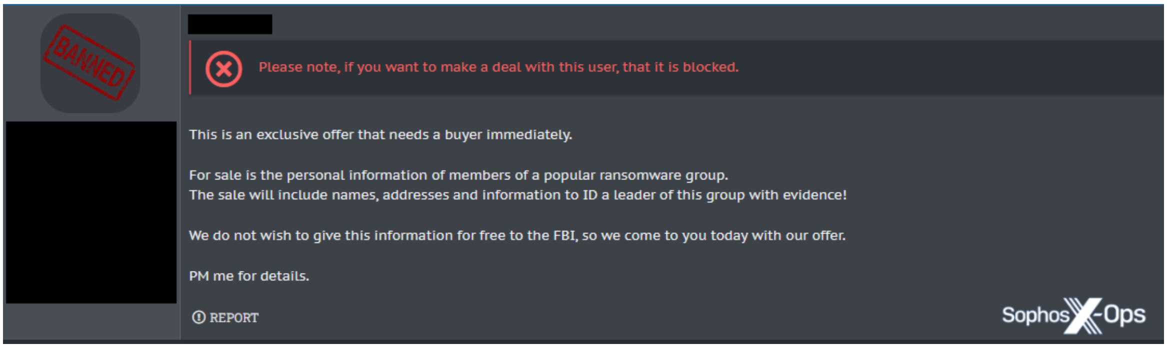
Figure 17: AsyncRAT advertised on a criminal forum in 2021

It's not just RATs, though; some threat actors go to more imaginative lengths to attack and disrupt rivals. In February 2022, for example, researchers uncovered a campaign involving malicious packages in the npm repository[44] – including one designed to attack other malware authors.

Earlier, we also mentioned threat actors sometimes close the door behind themselves, patching or removing the weakness(es) that they used to gain access. The Welchia worm famously did this in 2003;[45] it exploited the same vulnerability as the Blaster worm,[46] but once it was on a host, it downloaded a patch from Microsoft, fixed the bug, and attempted to remove Blaster infections – all without performing any (deliberately) malicious activity itself. Welchia is an example of a so-called 'helpful' worm, also known as an anti-worm, or nematode[47] – although, like almost all anti-worms, it poses significant legal and ethical risks. Welchia was also inadvertently harmful (though not destructive), causing denial-of-service conditions due to the amount of network traffic it generated.

More recently, our research into the Kingminer cryptominer botnet revealed that Kingminer checks if the infected system is vulnerable to the Bluekeep exploit, by enumerating the Windows version number and installed hotfixes. If no hotfixes are found, Kingminer disables any further RDP connections, to prevent other malware from exploiting the bug to gain access (even though Bluekeep was rarely abused by other cryptominers at the time).[48]

But as you might expect, given ransomware is a class of malware that has changed the face of security, it does things differently. That's not to say that ransomware groups always get along; they sometimes feud among themselves on criminal forums[49] and steal each other's code.[50] We've even seen threat actors trying to sell 'doxes' of a "popular ransomware group":



[redacted]

[redacted]

Please note, if you want to make a deal with this user, that it is blocked.

This is an exclusive offer that needs a buyer immediately.

For sale is the personal information of members of a popular ransomware group.
The sale will include names, addresses and information to ID a leader of this group with evidence!

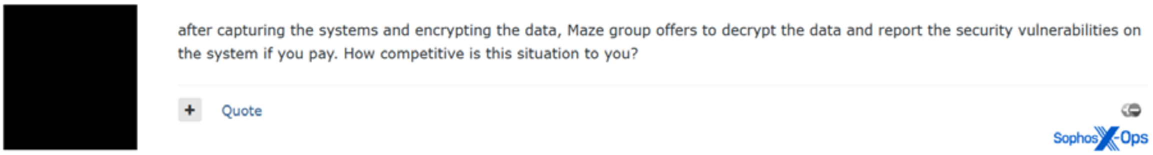
We do not wish to give this information for free to the FBI, so we come to you today with our offer.

PM me for details.

Figure 18: A (banned) user advertises personal information ('dox') of a ransomware group for sale on a criminal forum in 2020

But when it comes to attacks, they generally seem happy to share targets. They don't terminate rival ransomware processes, or kick other malware out, because they're not competing for CPU resources or botnet sizes – and they're not constrained by the need for long-term, undetected access. So there isn't really a need to 'kill the competition.'

In fact, when the Maze ransomware group[51] offered to point out security holes to paying victims, one user on a criminal forum asked: "How competitive is this situation to you?"



[redacted]

after capturing the systems and encrypting the data, Maze group offers to decrypt the data and report the security vulnerabilities on the system if you pay. How competitive is this situation to you?

Figure 19: A user inviting opinions on the Maze ransomware group's offer to notify victims of vulnerabilities in their networks after paying the ransom

Whether overlapping attacks benefit or disadvantage ransomware groups is another matter. On the one hand, anything that puts pressure on the victim to pay is a desirable outcome, from the threat actors' perspectives. We've seen various ways in which ransomware groups attempt to apply that pressure – some particularly unpleasant[52] – and it may be that multiple ransomware infections have a similar effect, though it doesn't seem to be a coordinated strategy.

On the other hand, multiple infections can complicate a ransomware actor's usual tactics (e.g., they can't threaten to leak data if it's been encrypted by another group[53]), and a victim faced with a double or even triple ransom may be more unwilling, or simply unable, to pay all of them. Ransomware groups might reason that the first to encrypt is more likely to get paid, so on a system with multiple ransomware infections, one group starting encryption may trigger others to follow suit. That could be one reason for some ransomware groups boasting about their encryption times.[54]

In our next case study, an organization was hit with three ransomware attacks, two of them within two hours.

Case study: Once, twice, three times encrypted

December 2nd 2021: A threat actor, possibly an IAB, establishes an RDP session on an organization's domain controller. The session lasts for 52 minutes.

April 20th 2022: A Lockbit affiliate gains access to the corporate network – likely through the exposed RDP instance, although, as we'll explain later, this is hard to determine – and exfiltrates data from four systems to **Mega**, a cloud storage service often used by threat actors.

April 28th: The threat actor moves laterally and executes **Mimikatz** to extract passwords.

May 1st: The threat actor creates two batch scripts to distribute a ransomware binary across the network via the legitimate tool PsExec.[55] Ten minutes later, the binary is executed on nineteen hosts, encrypting data, and a ransom note is dropped on each infected machine.

Less than 2 hours later: A Hive ransomware affiliate – again, probably using RDP for initial access – uses the legitimate tool PDQ Deploy[56] to distribute their ransomware binary across the network, using the command **C:\Windows\AdminArsenal\PDQDeployRunner\service-1\exec\windows_x32_encrypt.exe**. Around 45 minutes later, the binary is executed, encrypting data on sixteen hosts.

May 15th: An ALPHV/BlackCat[57] ransomware affiliate gains access to the network, moves laterally using compromised credentials, and drops two ransomware binaries. The binaries are distributed across the network using PsExec. Around 30 minutes later, the binaries are executed on six hosts, again encrypting data.

Less than 2 hours later: The ALPHV/BlackCat threat actor clears Windows Event Logs with the command **cmd.exe /c for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1"**. This action, along with some pre-investigation remediation actions and peculiarities in the organization's network configuration, will significantly complicate our incident response efforts. The BlackCat threat actor not only clears logs relating to their own activities, but also those of the Lockbit and Hive threat actors, making it difficult to determine the methods used for initial access, lateral movement, and other events.

May 15th: The Sophos Rapid Response team is engaged to assist, and observes three separate ransom notes, along with several double- and triple-encrypted files.

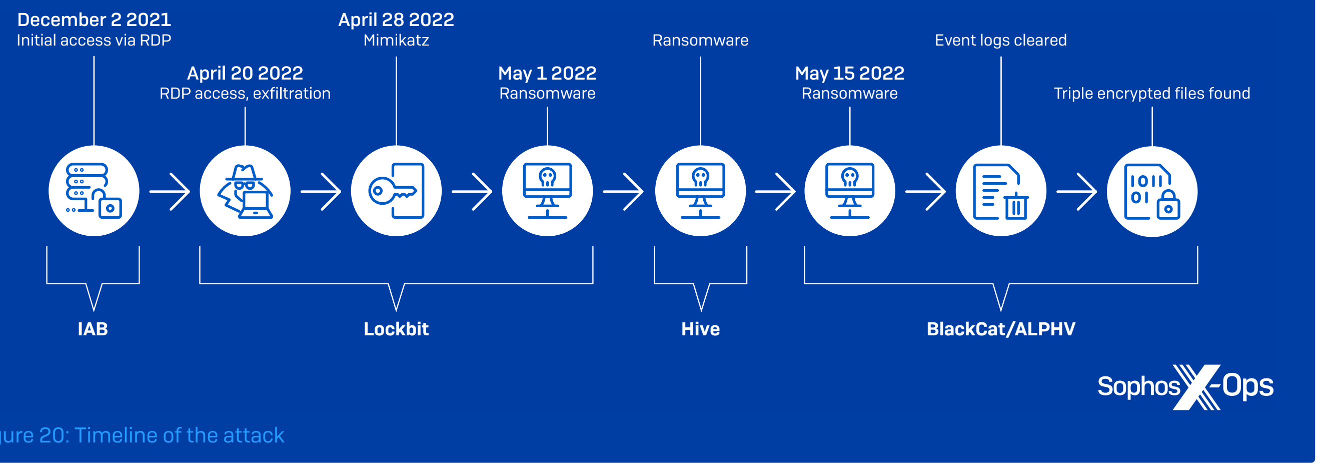
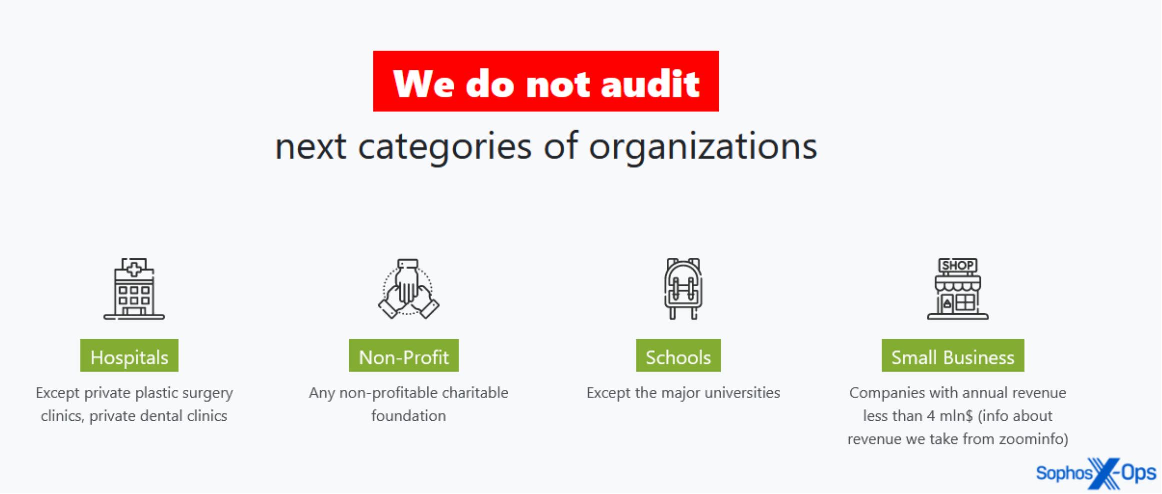


Figure 20: Timeline of the attack

It's possible that ransomware groups discuss these issues at a senior level – perhaps even working out mutually beneficial arrangements, so that, for example, when simultaneous infections occur, one group encrypts while another exfiltrates without encryption.

In fact, we observed exactly this behavior in a case from December 2021,[58] although we don't know if it was coordinated in advance.

First came a Karma ransomware infection via ProxyShell, but data was only exfiltrated, not encrypted (the ransom notes claimed that this was because the victim was a healthcare organization; other ransomware groups have stated they won't target certain kinds of healthcare businesses at all, as shown below). Then, as Karma ransom notes were still being dropped, along came Conti, via the same vulnerability – who did



We do not audit

next categories of organizations

Hospitals

Except private plastic surgery clinics, private dental clinics

Non-Profit

Any non-profitable charitable foundation

Schools

Except the major universities

Small Business

Companies with annual revenue less than 4 mln$ (info about revenue we take from zoominfo)

Figure 22: The Babuk ransomware group's rules, which forbid affiliates from attacking various categories of organizations, including hospitals

Whether they coordinate with each other or not, multiple attacks just don't seem to be a huge issue for ransomware groups. They may even accept it as an occupational hazard – a side effect of operating in an increasingly crowded and commoditized marketplace.

That said, ransomware actors do sometimes benefit from each other's activities when they attack the same organizations. From what we can tell, this isn't intentional – at least, not yet – but it does illustrate that responding to multiple infections can become more complicated for responders and investigators, as well as victims. In the following incident, a backdoor installed by one threat actor resulted in another attack, four months later.

Case study: Backdoor leads to another attack

January 6th 2022: Multiple attempts to exploit ProxyShell are discovered on an organization's network. Following initial access, a threat actor executes **Advanced IP Scanner**.

January 19th: The threat actor establishes an RDP connection to a compromised account. Throughout January and February, the threat actor makes several RDP connections and downloads RealVNC.[59]

February 23rd: Two devices on the network communicate with a C2 server over DNS. The threat actor exfiltrates over a terabyte of data to **Mega**. Over the next few days, the threat actor downloads and installs several legitimate tools, including WinScp,[60] an SFTP/FTP client; Rclone,[61] a cloud storage file manager; the compression utility 7-zip;[62] Putty,[63] an SSH and Telnet client; and AnyDesk,[64] a remote desktop application. Further RDP connections are established.

March 12th: The threat actor executes **AnyDesk**, and continues to download and install tools, including AdFind.exe[65] (an Active Directory query tool); SharpShares[66] (a binary which lists network share information); **lsass_dumper.exe**; and NanoDump[67] (which creates a minidump of the LSASS process). On the same day, the threat actor installs a **Cobalt Strike** beacon as a service, and executes a Base64-encoded PowerShell script to download and execute the legitimate penetration testing tool BloodHound,[68] used to identify potential attack paths in Active Directory.

March 17th: The threat actor drops and executes a Lockbit ransomware binary.

March 25th: Data from the organization is posted on Lockbit's leak site.

April 28th: A second threat actor enters the corporative environment via a publicly exposed RDWeb portal. They execute **rundll32 107s32.dll**, **StartW**, a command commonly used with **Cobalt Strike** DLLs, and several external connections are made to a **Cobalt Strike** staging server. This threat actor also attempts to download and execute **BloodHound**, but the activity is blocked.

June 2nd: A third threat actor abuses the previously installed **AnyDesk** instance to access the network and collect and exfiltrate credentials. They upload some of the organization's data to **dropmefiles[.]com**, a file-sharing service. The attack, from initial entry to exfiltration, takes less than fifteen minutes.

June 8th: 'Karakurt Team' contacts the organization with a ransom demand. Karakurt ('Black Wolf' in Turkish, referring to a spider found in Eastern Europe and Siberia) typically doesn't encrypt data, but steals and threatens to release it unless a ransom is paid.[69] Researchers have previously linked Karakurt to the Conti ransomware group.[70]

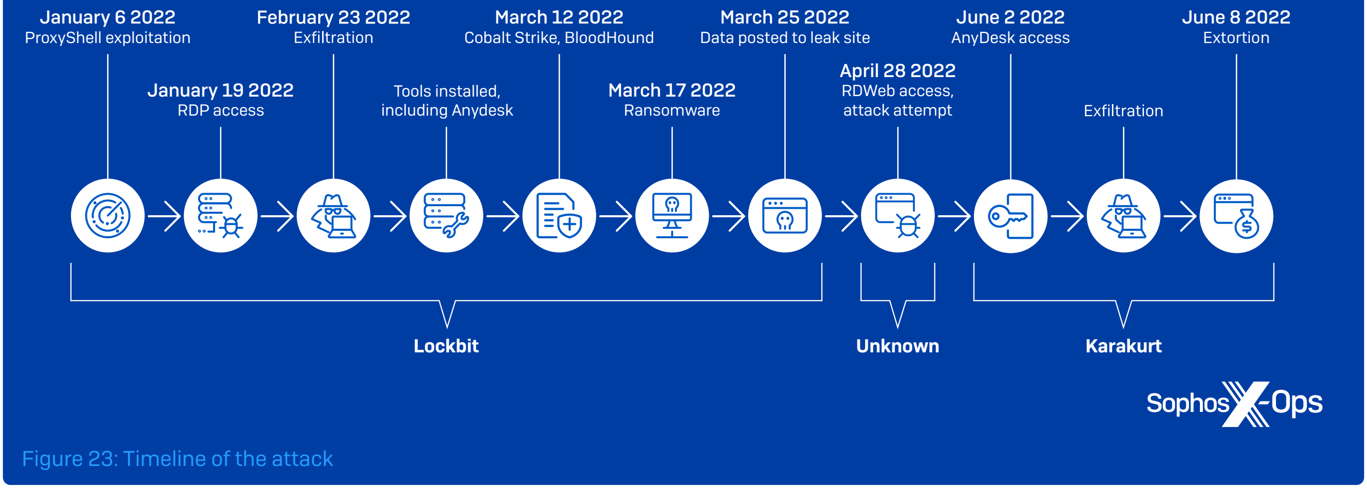


Figure 23: Timeline of the attack

Takeaway 6: Ransomware plays nicely with ransomware

Many threat actors have traditionally been competitive, to the point of kicking each other off infected systems, and that's still true today when it comes to cryptominers and some RATs. But ransomware doesn't seem to follow this trend, and may proceed to encrypt files even if other ransomware groups are on the same network – or operate in a mutually beneficial way, so that one group exfiltrates and the other encrypts.

Takeaway 7: Attackers open new backdoors

Some attackers may introduce further vulnerabilities after gaining access, or create deliberate or unintentional backdoors (including the installation of legitimate software), which a subsequent threat actor can exploit. So while it's crucial to close off the initial infection vector, it's also worth considering a) other weaknesses and misconfigurations that could be used to gain access, and b) any new ingress points that may have appeared.

Takeaway 8: Some attackers are worse than others

Not all ransomware strains are equal. Some have capabilities and features that may complicate attempts to respond to and investigate others – another reason to try to avoid becoming a victim of multiple attacks.

Guidance

So, are multiple attacks becoming more common? It's difficult to say with any statistical certainty, but anecdotally, signs point to an answer in the affirmative. As Sophos' Director of Incident Response, Peter Mackenzie, notes: "This is something we're seeing affecting more and more organizations, and it's likely due to an increasingly crowded market for threat actors, as well as ransomware-as-a-service (RaaS) becoming more professionalized and lowering the bar to entry."

As ransomware affiliate programs continue to recruit and expand, and cryptominers continue to take advantage of new vulnerabilities, the number of predators increases – and so do the number of opportunities.

In general, multiple exploitations are due to the victim not addressing the underlying cause of the initial attack. Other factors driving multiple attacks arise from features of the criminal ecosystem, but there are things organizations can do to avoid becoming a part of that ecosystem in the first place.

Along with the eight key takeaways we've included throughout this article, we recommend the following standard best practices to help defend against ransomware and related cyberattacks:

1. **Patch and investigate.** Keep Windows and other software up to date (and consider setting up some vulnerability alerts, and monitoring in-the-know sources, to get a head start on breaking news about new bugs). This also means double-checking that patches have been installed correctly and are in place for critical systems like internet-facing machines or domain controllers. However, this isn't just a case of applying patches quickly. Threat actors may leave backdoors – which may include the installation of legitimate software – or introduce new vulnerabilities, either deliberately or inadvertently, so this is a key thing for responders to look for to reduce the likelihood of a second attack.
2. **Monitor and respond to alerts.** Ensure the appropriate tools, processes, and resources (people) are available to monitor, investigate, and respond to threats seen in the environment. Ransomware attackers often time their strikes during off-peak hours, on weekends or during the holidays, on the assumption that few or no staff are watching.
3. **Lock down accessible services.** Perform scans of your organization's network from the outside and identify and lock down the ports commonly used by VNC, RDP, or other remote-access tools. If a machine needs to be reachable using a remote management tool, put that tool behind a VPN or zero-trust network access solution that uses MFA as part of its login.
4. **Practice segmentation and zero-trust.** Separate critical servers from each other and from workstations by putting them into separate VLANs as you work towards a zero-trust network model.
5. **Set and enforce strong passwords and multifactor authentication (MFA).** Strong passwords serve as one of the first lines of defense. Passwords should be unique or complex and never re-used. This is easier to do if you provide staff with a password manager that can store their credentials. But even strong passwords can be compromised. Any form of multifactor authentication is better than none for securing access to critical resources such as e-mail, remote management tools, and network assets.
6. **Inventory your assets and accounts.** Unprotected and unpatched devices in the network increase risk and create a situation where malicious activities could pass unnoticed. It is vital to have a current inventory of all connected computers and IoT devices. Use network scans and physical checks to locate and catalog them.
7. **Install layered protection to block attackers at as many points as possible.** Extend that security to all endpoints that you allow onto your network.
8. **Configure your products correctly, and check the configurations periodically.** Under-protected systems and devices are vulnerable too. It is important that you ensure security solutions are configured properly and to check and, where necessary, update security policies regularly. New security features are not always enabled automatically.

Acknowledgments

Sophos X-Ops would like to thank Hilary Wood and Colin Cowie of Sophos' Managed Detection and Response team; Syed Shahram Ahmed and Mauricio Valdivieso of Sophos' Rapid Response team; and Andrew Ludgate and Gabor Szappanos of SophosLabs, for their contributions to this report.

References

1 https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/

2 https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/

3 https://documents.trendmicro.com/assets/white_papers/wp-navigating-the-landscape-of-cloud-based-cryptocurrency-mining.pdf

4 https://nvd.nist.gov/vuln/detail/CVE-2021-26855

5 https://nvd.nist.gov/vuln/detail/CVE-2021-34473

6 https://nvd.nist.gov/vuln/detail/CVE-2021-34523

7 https://nvd.nist.gov/vuln/detail/cve-2021-31207

8 https://news.sophos.com/en-us/2021/03/17/MDR-in-real-time-exchange-proxylogon-edition/

9 https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/

10 https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/

11 https://news.sophos.com/en-us/2021/12/02/two-flavors-of-tor2mine-miner-dig-deep-into-networks-with-powershell-vbscript/

12 https://news.sophos.com/en-us/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud/

13 https://news.sophos.com/en-us/2021/03/15/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities/

14 https://news.sophos.com/en-us/2021/03/23/black-kingdom/

15 https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/

16 https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/

17 https://nvd.nist.gov/vuln/detail/CVE-2021-44228

18 https://news.sophos.com/en-us/2022/01/24/log4shell-no-mass-abuse-but-no-respite-what-happened/

19 https://news.sophos.com/en-us/2022/03/29/horde-of-miner-bots-and-backdoors-leveraged-log4j-to-attack-vmware-horizon-servers/

20 https://news.sophos.com/en-us/2022/06/16/confluence-exploits-used-to-drop-ransomware-on-vulnerable-servers/

21 https://nvd.nist.gov/vuln/detail/CVE-2022-26134

22 https://www.computerweekly.com/news/252510662/2021-another-record-breaker-for-vulnerability-disclosure

23 https://bugalert.org/

24 https://cvetrends.com/

25 https://www.advanced-ip-scanner.com/

26 https://github.com/gentilkiwi/mimikatz

27 https://www.cobaltstrike.com/

28 https://ke-la.com/access-as-a-service-remote-access-markets-in-the-cybercrime-underground/

29 https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf

30 https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild?view=vs-2022

31 https://twitter.com/GossiTheDog/status/1541688001620754436

32 https://twitter.com/vxunderground/status/1544306201600598016

33 https://twitter.com/vxunderground/status/1544306201600598016

34 https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf

35 http://news.bbc.co.uk/1/hi/technology/3532009.stm

36 https://nakedsecurity.sophos.com/2012/01/05/spyeye-bank-trojan-hides-its-fraud-footprint/

37 https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=6aa65e05-2a44-4dd3-be3d-6dbb06cc94ad&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

38 https://www.sophos.com/fr-fr/medialibrary/PDFs/technical-papers/Sophos-what-is-zeus-tp.pdf

39 https://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

40 https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp

41 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware

42 https://news.sophos.com/en-us/2022/05/30/follina-word-doc-taps-previously-unknown-microsoft-office-vulnerability/

43 https://nvd.nist.gov/vuln/detail/CVE-2022-30190

44 https://jfrog.com/blog/malware-civil-war-malicious-npm-packages-targeting-malware-authors/

45 https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf

46 https://docs.microsoft.com/en-us/troubleshoot/windows-server/security-and-malware/blaster-worm-virus-alert

47 https://www.youtube.com/watch?v=SrVeLNGcbBE

48 https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-labs-kingminer-botnet-report.pdf

49 https://www.techtarget.com/searchsecurity/news/252512902/Distrust-feuds-building-among-ransomware-groups

50 https://www.secureworks.com/research/lv-ransomware

51 https://nakedsecurity.sophos.com/2020/05/12/maze-ransomware-one-year-on-a-sophoslabs-report/

52 https://www.documentcloud.org/documents/20428892-doppelpaymer-fbi-pin-on-dec-10-2020

53 https://news.sophos.com/en-us/2021/08/11/ransomware-mishaps-adversaries-have-their-off-days-too/

54 https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

55 https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

56 https://www.pdq.com/deploy/

57 https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/

58 https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/

59 https://www.realvnc.com/en/

60 https://winscp.net/eng/index.php

61 https://rclone.org/

62 https://www.7-zip.org/

63 https://www.putty.org/

64 https://anydesk.com/

65 http://www.joeware.net/freetools/tools/adfind/index.htm

66 https://github.com/djhohnstein/SharpShares

67 https://github.com/helpsystems/nanodump

68 https://github.com/BloodHoundAD/BloodHound

69 https://www.cisa.gov/uscert/ncas/alerts/aa22-152a

70 https://www.infinitumit.com.tr/conti-ransomware-group-behind-the-karakurt-ha

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK

2022-08-01 EN (DD)

SOPHOS