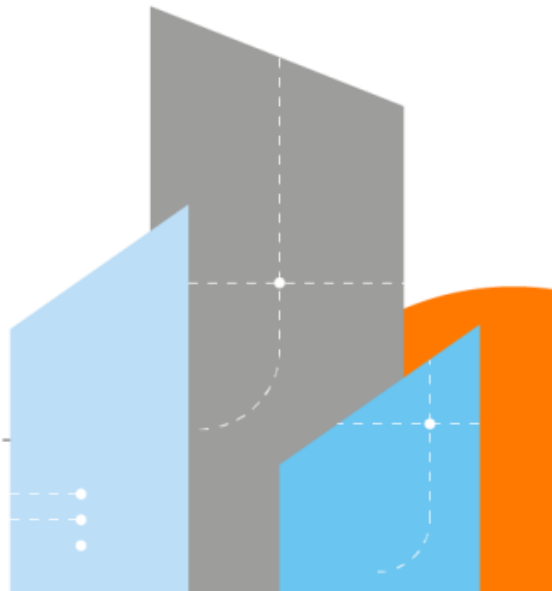
Orange
Cyberdefense

Security Intelligence

Quarterly Report

September 2022



CONTENTS

CONTENTS 2

INTRODUCTION 3

World Watch Review September 2022 4

Cyber Extortion Trends in Q3 2022 7

Editor's Notes 11

Passing through the eye of the needle 11

Very Bazar 13

Good News Cyber 14

INTRODUCTION

The UK National Cyber Security Centre (NCSC), alongside international allies, published an advisory warning of cyber actors affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC) exploiting vulnerabilities to launch ransomware operations against multiple sectors. The advisory outlines tactics and techniques used by the actors, as well as steps for organisations to take to mitigate the risk of compromise.

Australian telecommunications giant Optus disclosed details of a data breach, dubbed the worst in Australian history, impacting around 10 million customers. Optus revealed that current and former customers' data was stolen, including names, birthdates, home addresses, phone and email contacts, and passport and driving licence numbers. Payment details and account passwords were not compromised however according to the telecoms giant.

Microsoft released details of two zero-day vulnerabilities, initially discovered by Vietnamese cyber security company GTSC, affecting Microsoft Exchange Server. Active attacks targeting these vulnerabilities had also been detected. The new vulnerabilities have significant similarities to the previous critical zero-day, ProxyShell, seen in Exchange, leading security researcher Kevin Beaumont to dub them "ProxyNotShell". A patch is not yet available, although Microsoft have released, and regularly updated, manual mitigations to try and protect against the flaws.

Following the leak of the builder for the LockBit 3.0 ransomware strain by a disgruntled developer it was fully expected other ransomware groups would start to use it in their operations. This assumption has now been proven correct with the "Bl00dy Ransomware Gang" being detected using an encryptor built using the builder against a Ukrainian victim. Whilst this is the first detected use, it is surely only a matter of time before other threat actors follow suit.

Meta, the owner of Facebook and Instagram, said it has taken down an extensive Russian network spoofing more than 60 Western news sites to publish disinformation. The network was being used to publish articles criticising Ukraine and Ukrainian refugees, supported Russia and argued that Western sanctions on Russia would backfire. Meta reported that the network consisted of 1,633 accounts, 703 pages and one group on Facebook along with 29 accounts on Instagram.

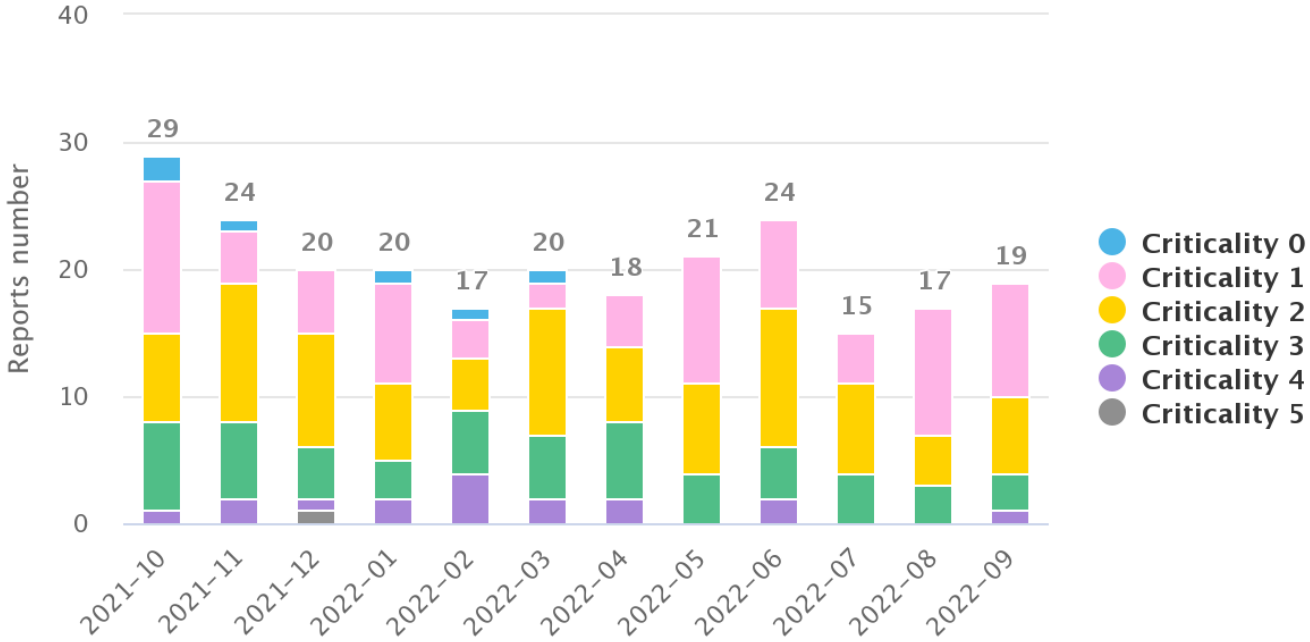
At a glance

The mitigations for the "ProxyNotShell" zero-day vulnerabilities in Exchange server continue to be regularly updated by Microsoft as researchers find ways to bypass them.

Despite October's Patch Tuesday having come and gone there are still no patches available for these vulnerabilities and, at the time of writing, no indication when any will be available.

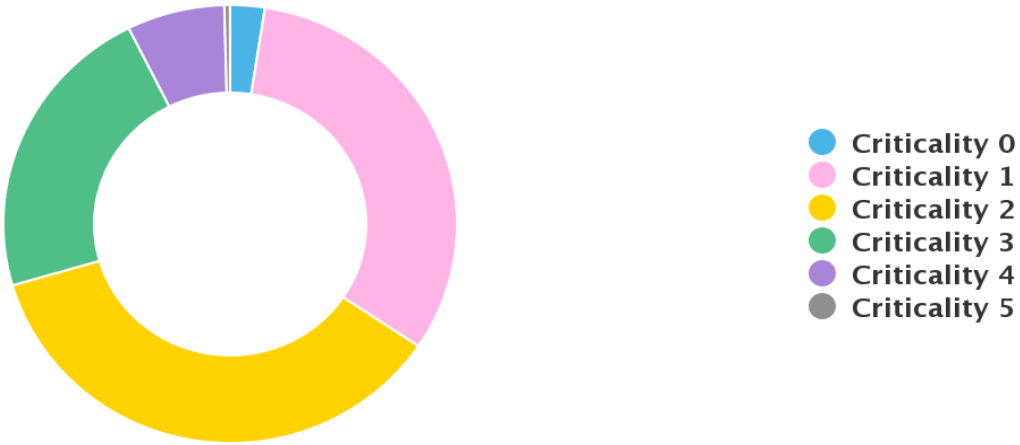
World Watch Review September 2022

The Orange Cyberdefense CERT published a total of 19 new World Watch advisories during September 2022, along with adding a further 27 updates to existing advisories. This volume of new advisories is another slight increase over the last 2 month's figures; additionally, the large number of updates published to advisories serves to highlight the work our CERT put in to stay abreast of any new developments as they arise and then communicate any relevant details to customers, including any changes in criticality or guidance.



Breakdown of Published Advisories Previous 12 Months

The criticality levels allocated to the majority of the September advisories again remained low. Although this month one advisory was given a criticality rating of 4, and three others were rated at 3.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As the charts above show the advisories this month were mostly given criticality ratings of Informational (1) or Low (2) when initially published, which follows the pattern for the last 12 months where more than two thirds of our advisories received the same ratings. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of initial publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially warrant a low rating, if for example there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase the reported criticality level as required if circumstances should change.

Some advisories of note this month are:

SIG-650623 - New ProxyShell-like Exchange 0-day RCE vulnerabilities actively exploited in targeted attacks

- On September 29, the Vietnamese cybersecurity firm GTSC issued a report warning that two vulnerabilities in Microsoft's Exchange server are being actively exploited in the wild. The report was issued 1 month after reporting the security vulnerabilities to Microsoft privately via the Zero Day Initiative program (at the end of August).
- These two vulnerabilities were tracked by Zero Day Initiative as ZDI-CAN-18333 and ZDI-CAN-18802, and presumably allow an attacker to gain access to the system, to drop webshells and to make lateral movements on the compromised network. According to the researchers, some of the systems compromised were fully patched against ProxyShell. Post-exploitation activity observed by the researchers mostly involved obfuscated webshells dropped on the Exchange servers.
- These attacks were performed with an exploit chain similar to those used in attacks leveraging the ProxyShell vulnerabilities.

SIG-648485 - Raccoon Stealer v2 aka Recordbreaker back among popular infostealers

- First (re)surfacing in June 2022 on XSS and WWH-Club, RecordBreaker is actually the newest version of the infamous Raccoon Stealer, a malware sold as a service which was not maintained anymore since March 2022 due to the invasion of Ukraine. As a result of the operation's suspension, threat actors had been reportedly massively moving towards alternatives such as the Mars, AgentTelsa, or various other stealers.
- Both the old and new malware strain of Raccoon offer fairly similar capabilities and features the same data stealing mechanism (i.e. base64 + RC4 encryption scheme for all string literals, and dynamic loading of WinAPI). But RecordBreaker differs from its predecessor in a certain number of aspects, notably after two successive updates in August:
    - RecordBreaker is written in C, unlike previous versions of Raccoon which were mainly written in C++.
    - RecordBreaker no longer uses the Telegram network to fetch a list of C2 servers. It now uses a hardcoded IP address of a threat actor-controlled server to fetch the list of C2 servers, from where the next stage payload (i.e. DLLs) is downloaded.
    - According to a recent technical report from CloudSEK, the newest version also possesses more effective anti-analysis and anti-debugging techniques to foil automated

analysis attempts. For instance, the packer notably makes use some variant of the anti-analysis trick called Read Time Stamp Counter (RDTSC).

SIG-648737 - Ongoing campaign distributing ChromeLoader and additional payloads detected

- In a new technical report published on September 19, VMware described at least ten ChromeLoader (a.k.a. Choziosi Loader according to GData or ChromeBack by GoSecure) variants that emerged since the first appearance of the malware, at the beginning of 2022. Seven of them appeared in the last two months, offering increasingly malicious features and demonstrating a clear offensive escalation attempt. As VMware researchers explain, as recent as late August, additional payloads have been seen being dropped onto infected systems:
  - ZipBombs, which destroy the user's system by overloading it with data if opened.
  - Enigma, an old ransomware strain using a JavaScript-based installer and an embedded executable so that it can be launched directly from the default browser.
- These highlight how ChromeLoader has evolved from regular adware to a more sophisticated payload offering infostealing and second-stage dropping capabilities. Its evolution illustrates how threat actors have been exploring more profitable alternatives than advertising fraud.
- The malware is currently distributed in an ongoing wide-ranging click fraud campaign, which was attributed to an unknown threat group, but tracked by Microsoft as DEV- 0796. Unfortunately, Microsoft did not release additional details about the targeted scope. VMware identified at least 50 of their clients running the Carbon Black EDR with ChromeLoader infections, in multiple verticals (i.e. thus not targeted at one sector).

SIG-647099 - Microsoft fixes actively exploited 0-day and 3 critical wormable vulnerabilities in September Patch Tuesday

- The vulnerability that is actively exploited is a privilege escalation one affecting the Windows Common Log File system driver, scored at 7.2 out of 10. While not many technical details about CVE-2022-37969 are available, Microsoft noted that the vulnerability has low attack complexity and requires no user interaction. Based on that, and with the fact that it already is exploited in the wild, we believe a PoC or exploit code will soon be publicly available, then heavily used by threat actors.
- Of the five critical vulnerabilities patched by Microsoft, 3 are wormable, meaning they can spread to further machines on the network without user interaction, like CVE-2022-34718. This vulnerability, which affects Windows TCP/IP could be exploited by an authenticated attacker by sending a specially crafted IPv6 packet to a Windows node where IPsec is enabled, achieving remote code execution on that machine. This vulnerability, although not exploited, is particular dangerous, since IPsec tunnels with IPv6 enabled is a very common configuration, be it for employees to access the internal network from remote locations (i.e. through VPNs) or to interconnect various internal and external networks.

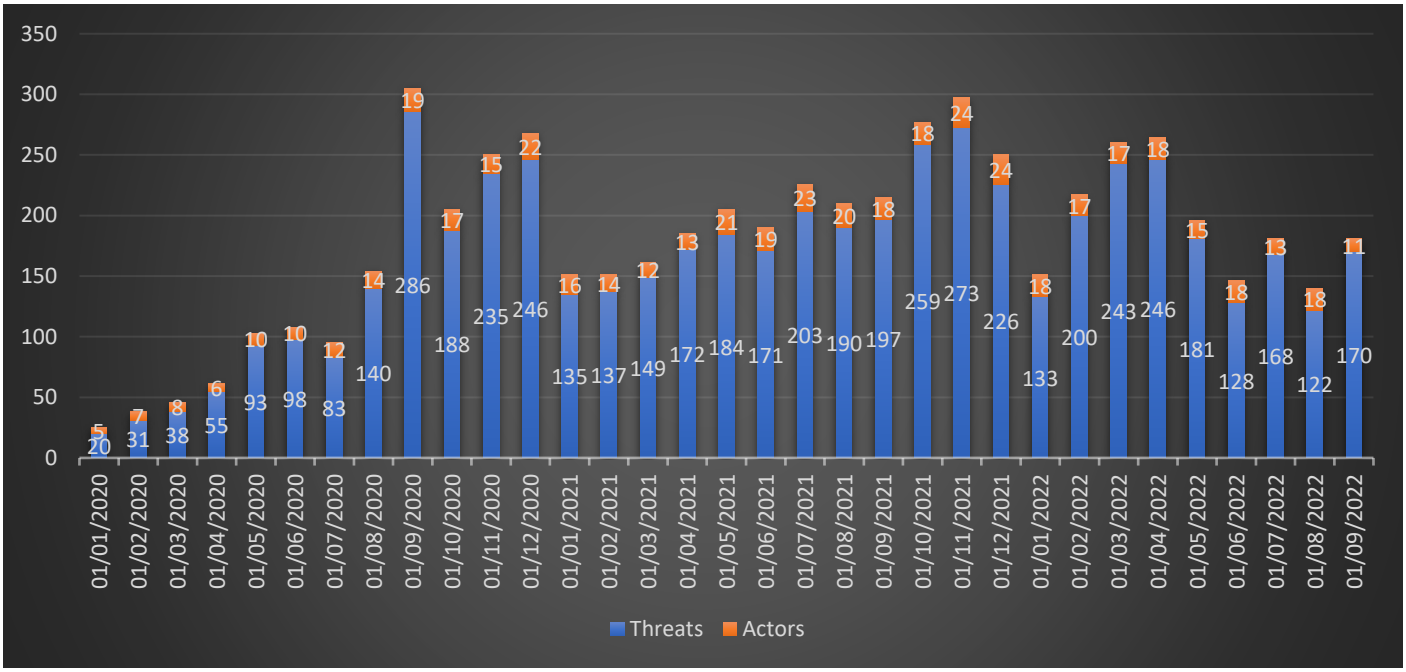
Cyber Extortion Trends in Q3 2022

Summary

- We recorded **460** businesses being victimized on cyber extortion leak sites during Q2
- In Q3, we saw a **decrease of 16%** in comparison to the previous quarter (Q2 2022, n=553)
- The top 5 cyber extortion groups contributing to the Q2 2022 victims were: LockBit2 (51%), Black Basta (11%), HiveLeaks (10%), ALPHV (aka BlackCat) (9%) and ViceSociety with 4%, Others (15%)
- During Q3, LockBit3 paid out its first Bug Bounty

General Trends

During Q3, we collected 460 victims off the so-called ransomware leak sites. In comparison to Q2, we saw a decrease of 16% (Q2 2022, n=553). Looking back one year, we see a decrease of 22% for this year's Q3 (Q3 2021, n=590). Q3 has seen the lowest number of victims for 2022 with August having only 122 victims. This could be due to Black Basta producing very few victims for this month along with other groups such as LV having their leak site disappear. Last quarter we commented on the void Conti has left and how this will be filled. From the data it looks like LockBit3 has taken a very large chunk of this with a market share of over 50%.



Extortion incidents & unique threat actor count recorded from 2020 to June 2022 (n=5,398)

Threat actor activity – Interesting observations

LockBit3.0 First Bug Bounty reward

On the 6th of July LockBit3.0 made its first bounty payment of $50,000 this was for a disclosure of a vulnerability in the encryption technique used. The vulnerability allowed for decryption of files where there are many known bytes. This is due to the key stream repeating every 128kb. If you find this key,

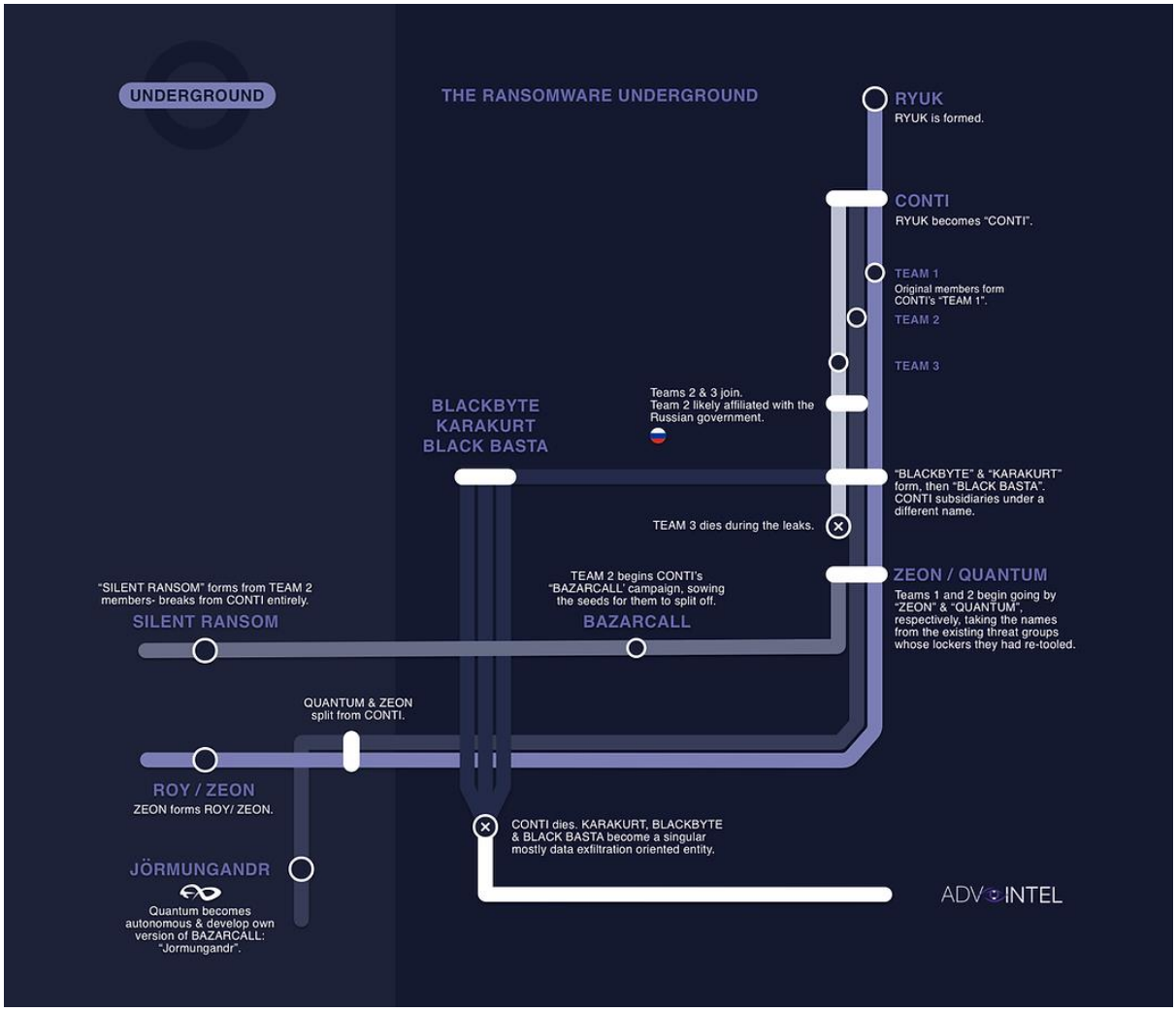
you can decrypt that specific file. This is easily done on files like virtual hard disks where there is a lot of zeros at the beginning.

In the post where the conversation between LockBit3 and the researcher takes place LockBit3 says that they built their code base upon BlackMatter. Lockbit3 initially said that they fixed the issues with the BlackMatter code but after the researcher showed that he could decrypt specific files, LockBit3 was more obliged to listen.

Where Did Conti Go

Ever since Conti shutdown operation there was speculation that they would rebrand or separate and join other ransom gangs. The graphic below from AdvIntel[1] shows that this is indeed true. Along with showing the various groups Conti members joined/formed it shows the different teams within Conti.

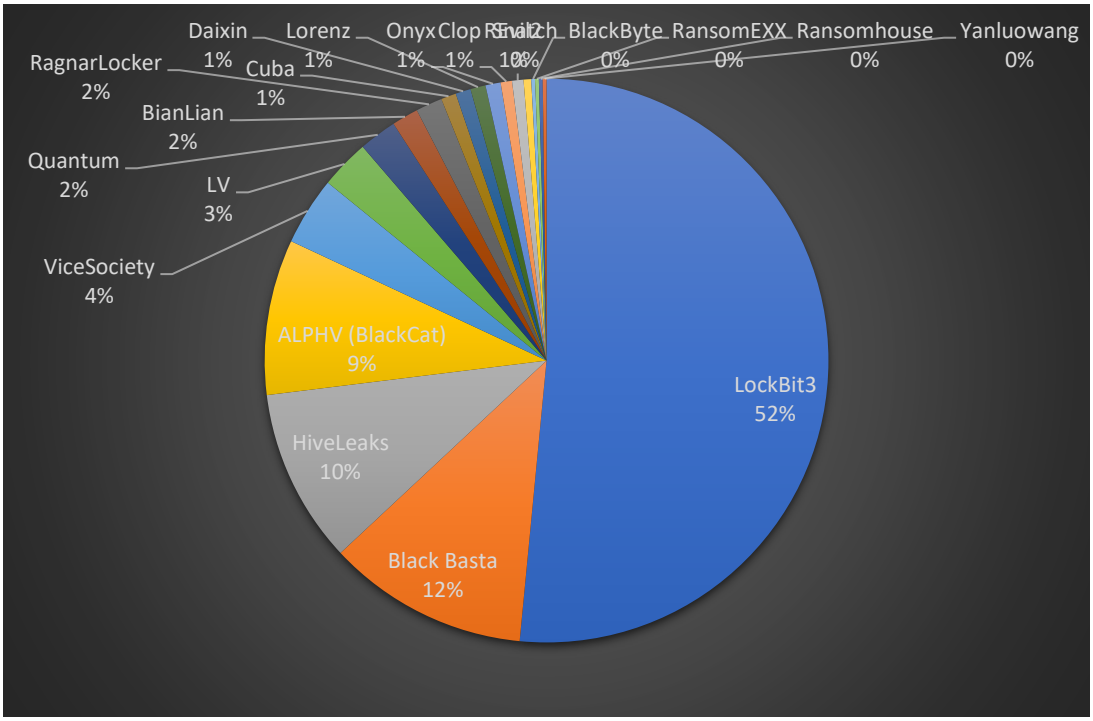
This shows that Teams 1 and 2 within Conti formed Zeon and Quantum whilst some of Team 2 formed Silent Ransom. Members from Conti also went on to Black Basta. When Conti was disbanded, the group dispersed widely moving to join/form many different Ransom gangs



[1] https://www.advintel.io/post/bazarcall-advisory-the-essential-guide-to-call-back-phishing-attacks-that-revolutionized-the-data

Victimology of Q3 2022

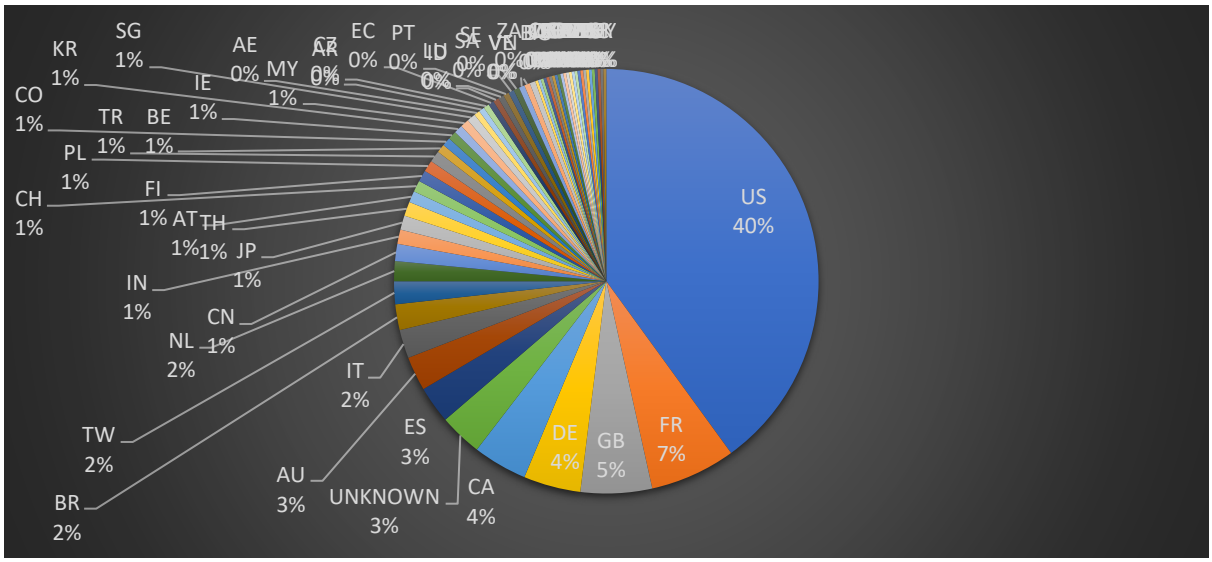
Q3 2022 has shown very similar numbers of victims being extorted on the so-called leak sites on the dark web. While we have observed changes in threat actor distribution, we saw an overall decrease in victims. During Q2, LockBit3 remained the top actor having the highest victim count with a share of 52%, followed by Black Basta with 12%. This group was first seen in Q2 and has been very active since. Apart from in the month of August where they did not post as much. The third most active threat actor in Q3 was HiveLeaks with a 10% share. For these 3 threat actors they all targeted US markets the most with LockBit3 having a high presence in the French markets.



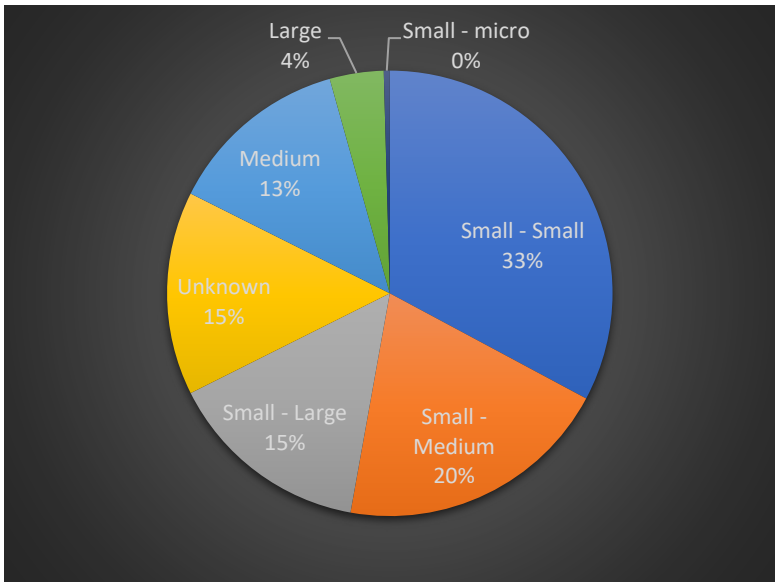
Contributors to cyber extortion leaks in Q3 2022

The countries that have been most impacted by this threat are the U.S., with 184 victim businesses, France (30 victims), United Kingdom (25 victims), Germany (20 victims) and Canada with 19 victims in Q3 2022. Spain, Australia, Italy, Brazil, and Taiwan are also represented in the top 10 impacted countries. This has not changed much from Q2 2022 With US markets being affected the most. France was targeted heavily this quarter by LockBit3 as seen in the data.

Victim organization's country in Q3 2022



Businesses most impacted by cyber extortion in Q3 were small organizations with an employee count varying from 1 to 999 (as can be seen below), accounting for almost 2/3 of all victims. Medium-sized businesses represented 13% of victims, and 18 businesses victimized with an employee count over 10,000 were registered during Q2 (4%). These large businesses originated from the Manufacturing sector (n=10), Management of Companies (n=4), Finance and Insurance (n=1), Information (n=1), Wholesale Trade (n=1) and Professional, Scientific, and Technical Services (n=1). The top three threat actor groups that compromised large organizations were LockBit3 (n=5), HiveLeaks (n=4) and Black Basta (n=2)



Size of businesses impacted by cyber extortion in Q3 2022

Business size classification

Small – Micro: 1-9 employees

Small – Small: 10-49 employees

Small – Medium: 50-249 employees

Small – Large: 250-999 employees

Medium: 1000-9,999

Large: 10,000+

Editor's Notes

Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

Wicus

Passing through the eye of the needle

In the August 2022 Editor's note I concluded that our businesses are complex and defending such complex infrastructure can be overwhelming. I also touched on the fact that architecting systems to fully use multi-factor authentication, least privilege, and segmentation are what will help contain a breach. This month we explore these aspects by looking at examples of recent breaches.

We'll start with the LastPass breach that was reported in late August 2022. The attacker managed to gain access to a developer's endpoint and used that to pivot into the LastPass development environment. This allowed the attacker access to parts of the development environment as well as access to proprietary information. LastPass did mention the access was limited to only that. LastPass' CEO Karim Toubba said that "our system design and controls prevented the threat actor from accessing any customer data or encrypted password vaults". From the official feedback, the attacker had access for four days to parts of LastPass's dev environment before the LastPass security team detected the anomalous activity.

A second example involves the recent network intrusion at Uber. According to The New York Times, that claims to have spoken to the attacker, they learned that an employee of Uber was socially engineered thus revealing their credentials. This was combined with the attacker spamming the multi-factor authentication push requests, known as MFA fatigue attack, for a period. Later the attacker contacted the victim convincing them they were from Uber IT, instructing the victim to accept the MFA push notification. MFA was in place preventing the attacker, but because the attacker leveraged the constant push notification to irritate the victim plus using the ploy of IT support fooled the user enough. From reports it seems that the attacker obtained access to sensitive proprietary information, such as vulnerability reports, as well as important IT systems.

The next two examples involve breaches at gaming companies, Rockstar and 2K, both owned by the same parent company Take-Two. Rockstar announced that an attacker managed to gain access to proprietary information relating to a project for an upcoming game, GTA 6. While 2K's customer helpdesk platform was compromised resulting in phishing emails being sent to victims that contained an info stealing malware. The Rockstar incident is allegedly linked to compromised Slack and Atlassian Confluence wiki accounts. It is unclear if the attacker was on the inside of the Rockstar's network or merely had remote access to the aforenoted services. The 2K helpdesk compromise involves a compromise of credentials of a third party associated with 2K. The attacker used this access to launch a phishing attack with a malicious information stealing malware attachment included.

Finally, we look at the breach involving Australia's second largest mobile operator, Optus. An attacker claimed to have stolen 11 million customer records from Optus by accessing an API endpoint. Unlike the other examples, there was no credential

theft or MFA shenanigans involved in this breach. For some reason Optus left the API exposed to the Internet with no protection. Anyone with basic web programming skills could query the API. The only effort required, it seems, was that the attacker had to enumerate, which is a very common attacker technique, certain parameters in the API to find legitimate client records. To put it in perspective, the only way Optus could have made this easier for the attacker was if it left a file containing all the client information on a web server for the attacker to download.

In the LastPass example with the compromised endpoint, one could wonder if this was targeted. We have seen many reports of targeted social engineering attacks where attackers place fake developer job adverts and then get their victims to install malicious software or open malicious documents as part of the interview process. This in turn gives the attacker a foothold on that developer's environment to pivot where the attacker wants.

The attacker behind the Rockstar incident also claims to have been responsible for the Uber breach. Subsequent reports indicate that the UK authorities have arrested an underage UK man for allegedly being linked to these incidents. Uber went as far as to attribute their latest breach to Lapsus$, the same group behind the Okta breach. The 2K breach also involved compromised credentials, possibly through phishing, but it's not clear if the Rockstar breach is related. My guess is these two are unrelated because in the 2K incident follow on actions involved further phishing with malware. The Uber and Rockstar incidents only saw data leakage.

Companies consists of lots of moving parts and keeping track of these are challenging to say the least. The examples shared above mainly talk to compromised access and the human element, with exception to the Optus breach. I speculate that Optus neglected to perform penetration testing on the API or failed to act on feedback from such consultancy. The mere fact that one could enumerate client records is proof that there was little regard for basic security. The Uber breach does raise concern as it seemed the one account compromised allowed the attacker to pivot to many sensitive areas of the business. It is sad to see that breaches even affect those companies that follow industry best practices by having authentication with MFA.

MFA fatigue attacks made the headlines as far back as early 2021. This prompted identity providers to strengthen their products to support challenge response whereby the user must select the code displayed on their mobile app after they accepted the push notification. I think that this may not be enough. If the fake "Uber IT" support guy can contact their victim convincing them to accept the push notification, then our attacker can also convince their victim to divulge the code.

Phishing resistant hardware tokens that are FIDO2 compliant may be a better solution, for one there is not pop up appearing on the victim's phone. These tokens require proximity to the device performing the authentication request as well as physical interaction. Additionally, the hardware token with the application, for example a web browser, can verify that the request is coming from a legitimate URL, unlike the popup appearing on the mobile application. This type of

authentication token is highly recommended for privileged accounts with access to sensitive systems and/or information.

Securing credentials and managing access to resources is hard. Doing it so that your employees can be productive without putting them into compromising positions is even tougher. The true cost of doing secure business on the Internet seems to be climbing higher.

Joshua

Very Bazar

Can you think of common ways initial access is gained for ransomware gangs? It could be mass phishing attacks with malicious Microsoft office macros or malicious lnk files. That would be a very good guess but, I doubt you were thinking of a tech support scam spin off called BazarCall.

So, in a nutshell what happens is, emails are sent to victims impersonating a company/person and within the email there is an urgent reason to call the number within the email. This could be to unsubscribe or to get a refund etc. Once the number is called they persuade the victim to install some form of remote access tool and from there they will generally execute a C2 payload.

Let's look at an example of PayPal being impersonated. An email from PayPal saying your account got hacked and $400 has been debited from your account. It says on the email to immediately contact us and provides a phone number. What is interesting is that the email is PayPal's email address, and they are abusing the invoice functions in PayPal to send people invoices with messages attached.

Now why would threat actor's employ these tactics when they must maintain a call centre and people to perform social engineering, when they could just mass spam malicious files and hope to infect an organization? The reason these tactics are used is that they have a higher conversion rate to access, because of this, attacks are becoming more targeted so they can attempt to infect specific employees at a specific organization. The attacks also are very specialised to help lure the victim in. Based on their job and other public information they can personalise an email they would be most likely to fall victim to.

This leads to some interesting insights. Industries attacked by ransomware before this technique was employed were more randomised. When this technique was regularly employed patterns would become more apparent. Such as the targeting of manufacturing and the finance sector. Overall, this initial access method is regularly utilised by the descendants of Conti and has shown that threat actors will go to any lengths to get better returns for their efforts.

Good News Cyber

Microsoft's latest enterprise release of the Windows operating system, release Windows 11 22H2, has a new feature called Enhanced Phishing Protection. This feature aims to limit the potential exposure of credentials typically because of phishing attacks, reuse, negligence, or user error. This seeks to help protect users that still rely on username and password to authenticate. The Enhanced Phishing Protection feature can detect if enterprise passwords are typed into another application or website. Microsoft Defender for Endpoint can also detect if the enterprise password is saved using WordPad, Notepad, or Office applications.

The European Commission proposed new legislation called the Cyber Resilience Act (CRA) and aims to regulate the cybersecurity of "products with digital elements" sold in the European Union. The CRA will not be applicable to "free and open-source software developed and supplied outside of commercial activity", nor does it apply to medical devices for human use. Device manufacturers will need to provide security updates for products for a period of five years. Fines for non-compliance can be up to €15m or 2.5% of annual gross profit for the preceding year, whichever is higher.

The U.S. government is ramping up to "disrupt specific ransomware actors". A kick-off meeting of the Joint Ransomware Task Force (JRTF) was attended by CISA, the FBI, Department of Justice, cybersecurity companies and other members of the private sector. The JRTF is a project launched by the U.S. Congress to fight the scourge of ransomware. In this first meeting members focused on setting primary goals to focus their efforts on.

Three former NSA employees were banned from participating in any activity relating to foreign commercial surveillance as well as fining the three a combined total of $1.7 million. The three ex-NSA employees were implicated in Project Raven that supplied surveillance capabilities to states such as United Arab Emirates. The U.S. State Department ruled the three individuals were guilty of transgressing International Traffic in Arms Regulations.

A seventeen-year-old man from the United Kingdom was arrested by City of London Police in connection with cyberattacks against Rockstar Games and Uber. The man was previously arrested in March 2022 for his alleged involvement in the Okta breach, which means the involvement of the cybergang known as Lapsus$. The man pled innocent on the arrest charges but did acknowledge he breached his bail conditions and is now held in a juvenile detention center.