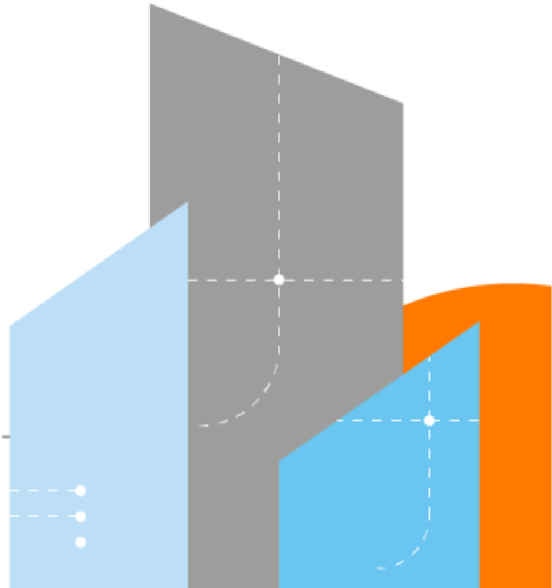
Orange
Cyberdefense

Security Intelligence

Quarterly Report

June 2022



CONTENTS

INTRODUCTION

Welcome to the quarterly report for Q2 2022, in this quarterly version of our report we strive to provide some extended information and details of research and work we are carrying out.

We have an overview of the Cyber Extortion Trends for Q2 2022 which comes from our analysis, and enrichment, of data from the cyber extortion leak sites.

There is also a “Tales from the Trenches” update which comes from the newly formed Advanced Intelligence & Detections team who are based out of Malmo. This update focuses on the work they are doing to track post exploitation frameworks and other malware.

We also provide an overview and analysis of the Verizon Data Breach Incident Report for 2022. The DBIR report celebrates its fifteenth year having first been published in 2008. Over these fifteen years the DBIR team examined 914,547 incidents and 234,638 breaches.

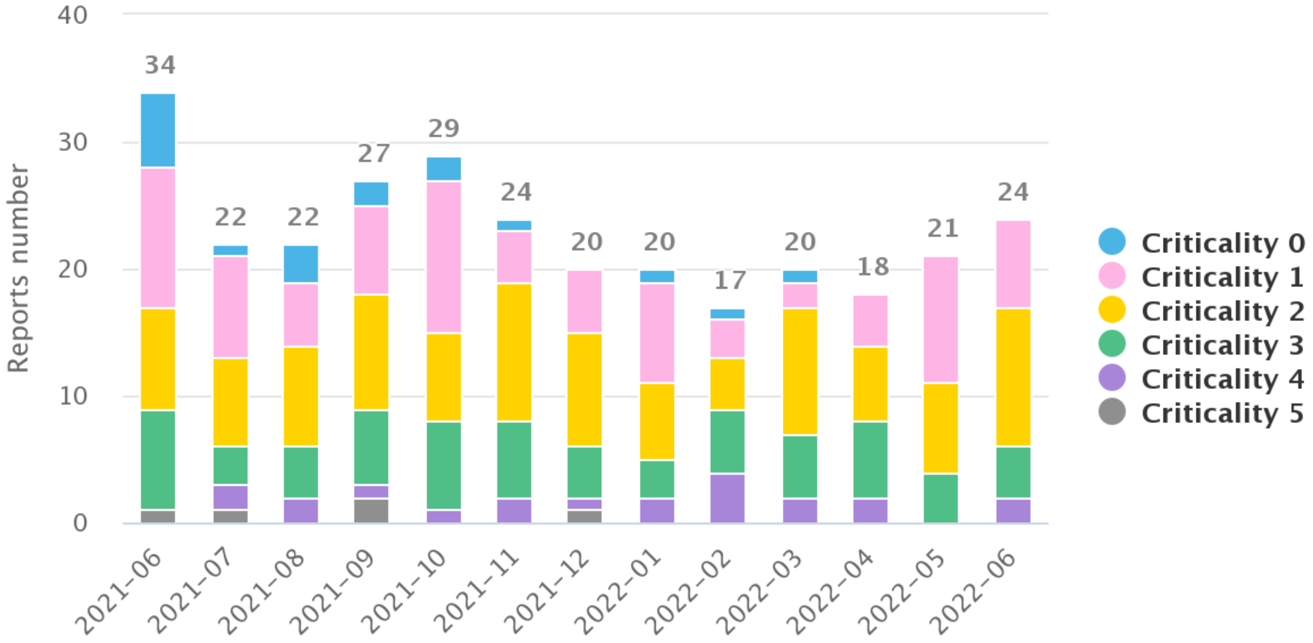
At a glance

We recorded 553 businesses being victimized on cyber extortion leak sites during Q2.

In Q2, we saw a decrease of 2% in comparison to the previous quarter (Q1 2022, n=563).

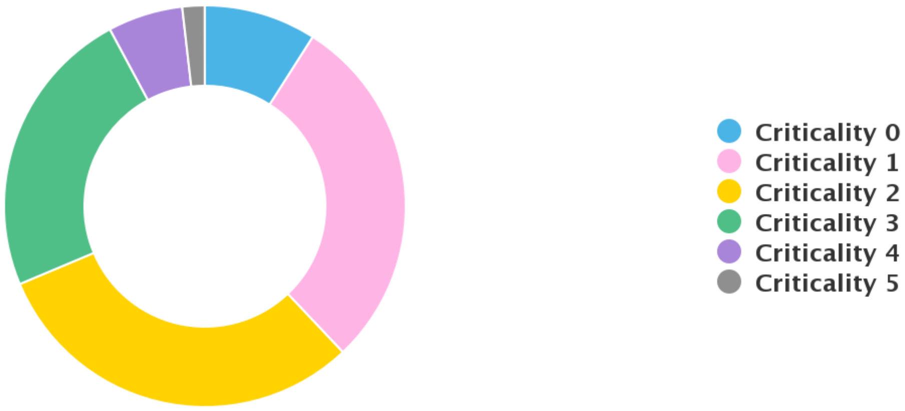
World Watch Review June 2022

The Orange Cyberdefense CERT published a total of 24 new World Watch advisories during June 2022, along with adding updates to a further 23 previously published advisories. June has been the busiest month of 2022 so far for new advisories, with Q2 showing a relatively steady increase month on month.



Breakdown of Published Advisories Previous 12 Months

The Criticality allocated to the June advisories was again primarily low, although two advisories this month were allocated a Criticality rating of 4, one of these was a manual archive of the existing advisory regarding the war in Ukraine however.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As can be seen above, apart from two, the advisories this month were all given criticality ratings of low or medium when initially published. 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 publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase our criticality level as required if circumstances should change. Some advisories of note this month are:

SIG-614909 - Exploit and patch available for Confluence pre-auth RCE vulnerability

- On June 2, 2022, Atlassian published a security advisory for CVE-2022-26134, a critical unauthenticated remote code execution vulnerability impacting both Confluence Server and Data Center. Using this vulnerability, a remote attacker can send a specially formed request to the server to execute arbitrary code with root privileges. On June 3, Atlassian released security updates to address CVE-2022-26134, a critical unauthenticated remote code execution vulnerability impacting even more versions than initially thought, i.e., all Confluence Server and Data Center versions after 1.3.0. Fixes have been released to solve this issue, in versions 7.4.17 (LTS), 7.13.7 (LTS), 7.14.3, 7.15.2, 7.16.4, 7.17.4 and 7.18.1. Atlassian recommends that you upgrade to the latest Long Term Support (LTS) release. Alternatively, the vendor also proposes a temporary mitigation technique intended for admins who cannot immediately upgrade their Confluence instance. The workaround consists of replacing .jar and .class files on the Confluence server by following the detailed instructions available in the Atlassian advisory.

SIG-619043 - Hertzbleed remote side-channel attack affects most modern x86 processors

- A team of academic researchers from three US universities recently disclosed a new family of side-channel attacks targeting x86 processors. Dubbed Hertzbleed, or frequency throttling side channel, this technique allows turning power side-channel attacks, which normally require physical access, into remote timing attacks. In the worst case, these attacks can allow an unprivileged attacker to extract cryptographic keys from remote servers. According to Intel's advisory, all of its processors are vulnerable to this attack technique. AMD's advisory reveals that most AMD processors released after 2017 are also vulnerable. Some ARM processors that use frequency scaling may also be vulnerable, but the researchers have not confirmed if that is the case, and the vendor has not released an advisory despite being made aware of the paper.

SIG-614497 - Fortinet details a new phishing campaign distributing three different malware

- Fortinet has detailed a phishing campaign targeting Microsoft Windows users with AveMariaRAT, BitRAT and PandoraHVNC trojans. The campaign allows cyber criminals to steal usernames, passwords and other sensitive information, including bank details. The initial phishing message seems like a payment report from a trusted source, with a short request to open an attached Microsoft Excel document. The most dangerous part about the email is that it automatically triggers the malware when you open the document and enable macros. The macro command fetches the three malware variants from the cybercriminal's server, disguised as a legitimate PowerShell file, to bypass detection.

SIG-614967 - Sophisticated threat actor LuoYu performs man-on-the-side attacks

- On June 2, Kaspersky released a new article on the threat actor LuoYu and on its recent arsenal. Active since 2008, LuoYu is a lesser-known Chineses-speaking threat actor which interestingly primary goes after targets located in China. The group leverages malware strains such as SpyDealer, Demsty and WinDealer and is able to both perform man-on-the-side attacks and use SIGINT as attack vector. In recent campaigns, LuoYu managed to infect its victims by switching legitimate app updates with malicious payloads. It is considered by Kaspersky as an extremely sophisticated threat actor.

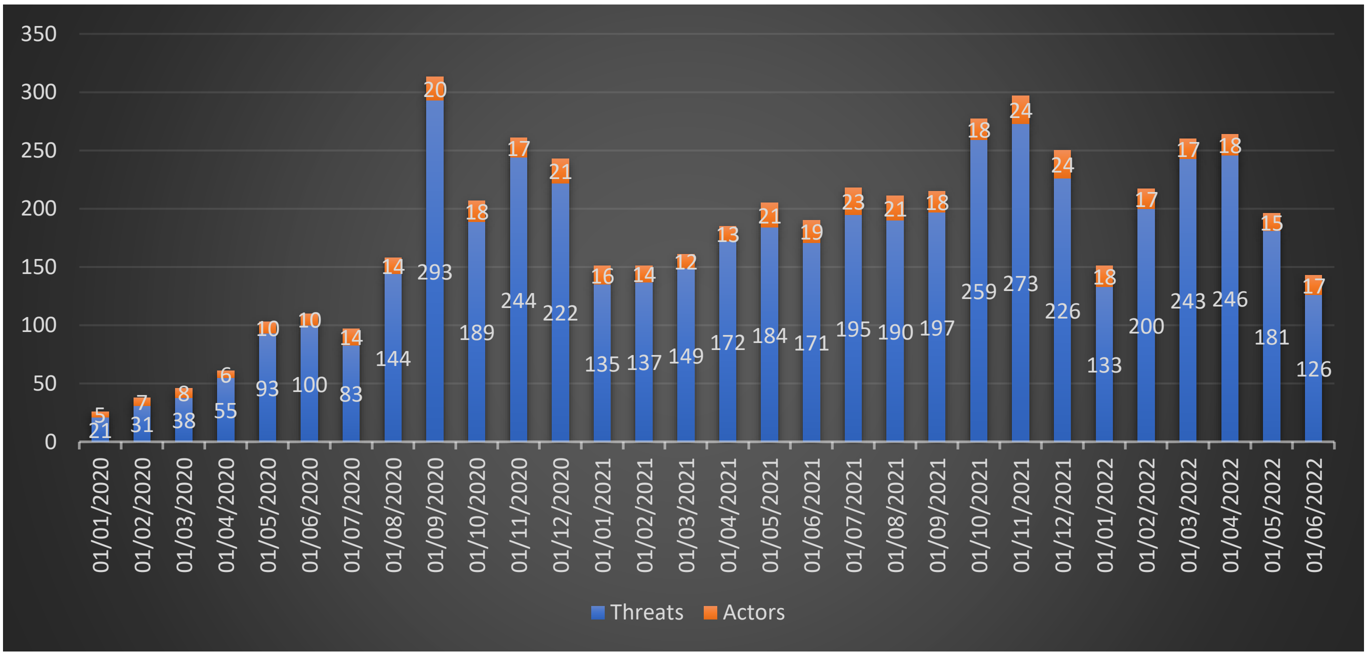
Cyber Extortion Trends in Q2 2022

Summary

- We recorded **553** businesses being victimized on cyber extortion leak sites during Q2
- In Q2, we saw a **decrease of 2%** in comparison to the previous quarter (Q1 2022, n=563)
- The top 5 cyber extortion groups contributing to the Q2 2022 victims were: LockBit2 (38%), Black Basta (11%), ALPHV (aka BlackCat) (9%), Conti (9%) and ViceSociety with 7%, Others (26%)
- During Q2, Costa Rica suffered severe cyber attacks, declaring a state of emergency

General Trends

During Q2, we collected 553 victims off the so-called ransomware leak sites. In comparison to Q1, we saw a decrease of 2% (Q1 2022, n=563). Looking back one year, we see an increase of 6% for this year's Q2 (Q2 2021, n=521). Nevertheless, Q2 has seen the peak of 2022 victims so far in April with 246 businesses being extorted; and at the same time it has seen the lowest volume of cyber extortion victims of 2022, in June. One potential reason for this is that the threat actor group Conti shut down its operations in June and thus the number of victims has gone down significantly. At the same time, LockBit2 has developed into LockBit3 causing a few days of low activity. As we usually observe, new threat actors have quickly filled in the voids left when established groups cease operations. A new threat actor for Q2 is Black Basta, who we first started monitoring in late April 2022.



Extortion incidents & unique threat actor count recorded from 2020 to June 2022 (n=4,938)

Threat actor activity – Interesting observations

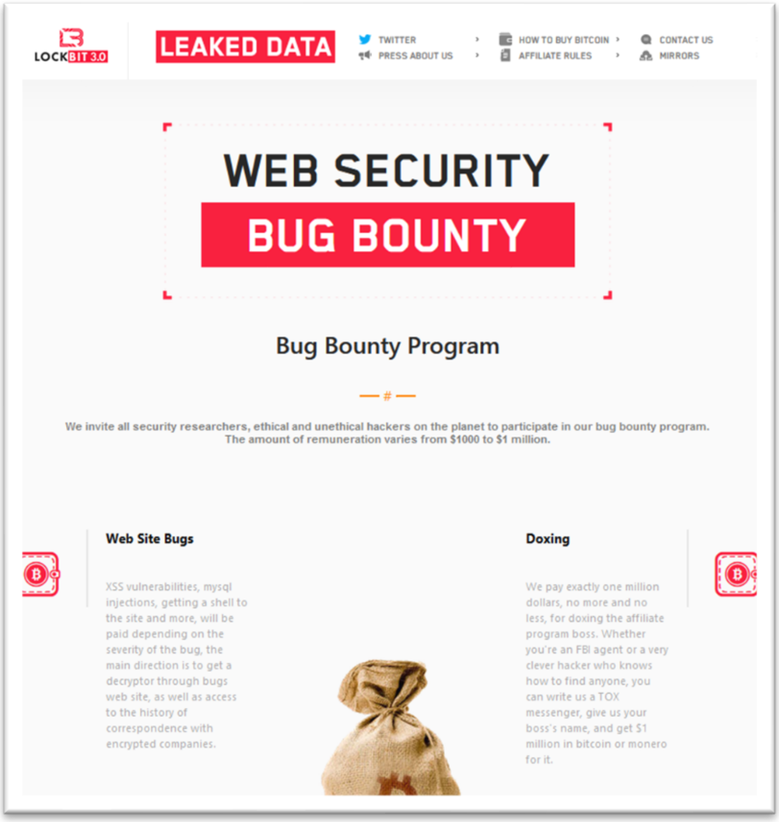
Conti & Costa Rica

In the beginning of May 2022, the newly elected Costa Rican President Chaves had to declare a national emergency due to an ongoing ransomware attack from the threat actor group Conti that started in April. By the end of May, the attack had impacted 27 institutions, including municipalities and state-run utilities.

The timing of the attack was very unusual and one might wonder how coordinated this was. Generally speaking, the main motivation for those groups is financial gain. But at the same time, it cannot be denied that this attack caused not only financial loss but also disruption and a threat to Costa Rica.

Raising the initial ransom demand and setting a time limit on the availability of the decryption key is a typical technique used by cyber extortion groups to increase pressure on their victims. Conti has been very successful using this technique and is one of the only threat actor groups that has overcome internal challenges to their criminal organizations (two internal breaches within several months). Active since June 2020, the group has also had a longer-than-average lifespan for a cyber extortion group – Other threat actor groups tend to be in operation for a short period of time and then quickly disappear or rebrand. The U.S. State Department has announced a reward for any information on the Conti group. In June, Conti has shut down its operations, but rumours say that the group is about to break down into several smaller criminal units. But until now, no proof of this has been provided. If this is true, it is a very common pattern for those groups who have had high profile victims and afterwards went offline. This was seen with DarkSide after the Colonial Pipeline attack and REvil after attacking the managed service provider Kaseya last July. Unfortunately, these groups never really cease operations; they either rebrand or lay low for some time before they resurface.

LockBit 2 has published its 3.0 version including their own Bug Bounty program



WEB SECURITY
BUG BOUNTY

Bug Bounty Program

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million.

Web Site Bugs

XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decryptor through bugs web site, as well as access to the history of correspondence with encrypted companies.

Doxing

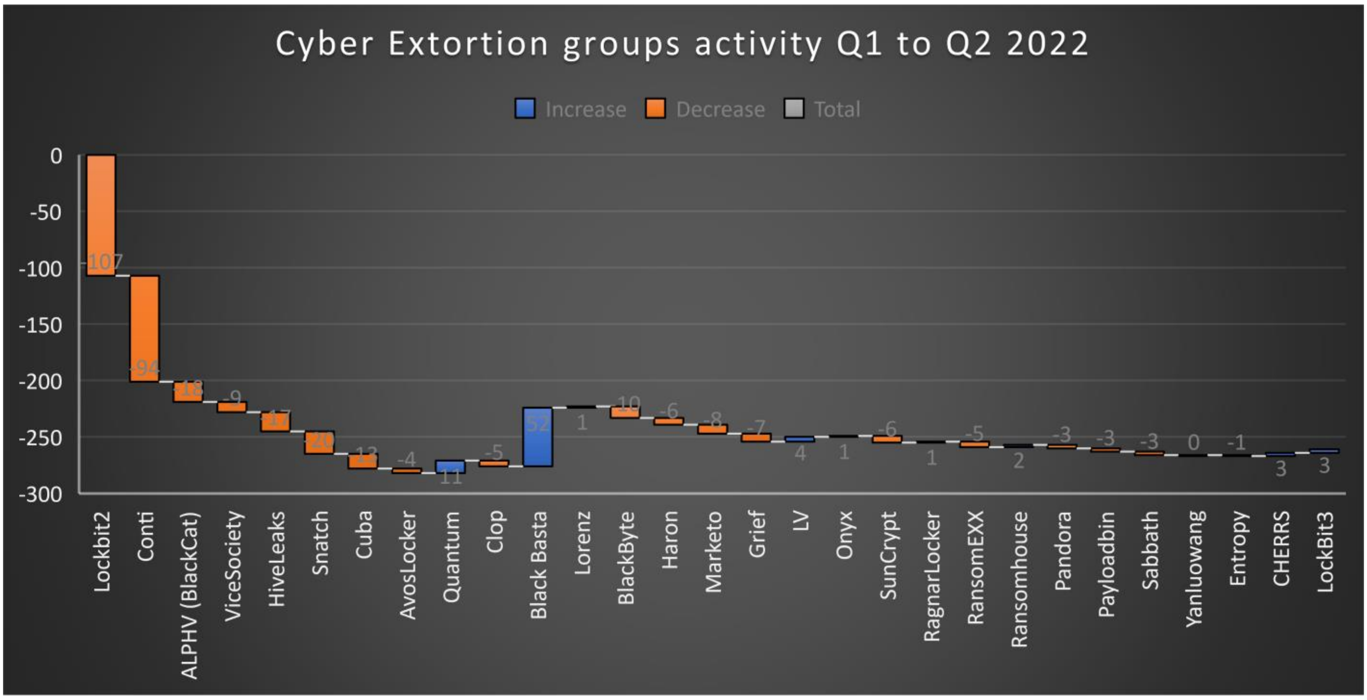
We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.

In late June, LockBit2's leaksite underwent changes and started re-directing to the new page of LockBit3. While in the beginning both versions were still accessible, with LockBit2 containing all extorted businesses posted during the LockBit2 time; the new page of LockBit3 started fresh, with a new victim list. At the time of writing, the LockBit2 page is offline and all onion sites re-direct to the new page of LockBit3.

Up until today, we have documented over 897 businesses that were victimized by this threat actor group. While this is a fairly large number of victims, we know that there is also a significant 'dark number' of victims who have come to an agreement with the threat actors and thus did not show on the extortion leak site.

There are several new features on the site. One of them is a new sub-page called "Web security & Bug Bounty". It is exactly what it sounds like – LockBit3 has come up with their own bug bounty program, encouraging 'researchers, ethical and unethical hackers on the planet' to submit potential vulnerabilities in LockBit's website and ransomware, as well as potential identities of the group's leader and ideas on improvements. Another feature that was added to the new site are different payment options directly accessible at each leak. These payment options are available for anyone interested in the data, as well as the victim organization itself. Options available are: 1.) Extend timer for 24 hours (costs = $10,000); 2.) Destroy all information (costs = $30,000) or 3.) Download data at any moment (costs = $30,000). The costs can vary from victim to victim. Since the site of LockBit3 was published at the end of June, we have registered 13 new victims. Unfortunately, it seems that LockBit3 will have similarly high volumes of victims posted as its previous leak page.

Based on the above-described threat actor activities of both groups, Conti and LockBit3, we have seen less activity during June 2022. If we compare the count of victims posted by each group in Q1 2022 with Q2, we see that two of the most active threat actor groups have seen significant decreases, causing the low number in June. During the Q2 period, we registered a new cyber extortion group called ‘Black Basta’. Black Basta appeared first during late April, and has since then picked up on victimizing businesses in the U.S., Germany, Canada, Switzerland, France and Italy. Other threat actors with an increase in Q2 in comparison to the previous quarter are the older groups Quantum (+11 victim) and LV (+4); in addition to Ransomhouse (+2), who only appeared in April, and CHEERS (+3 victims) who was only added to our tracking in June.

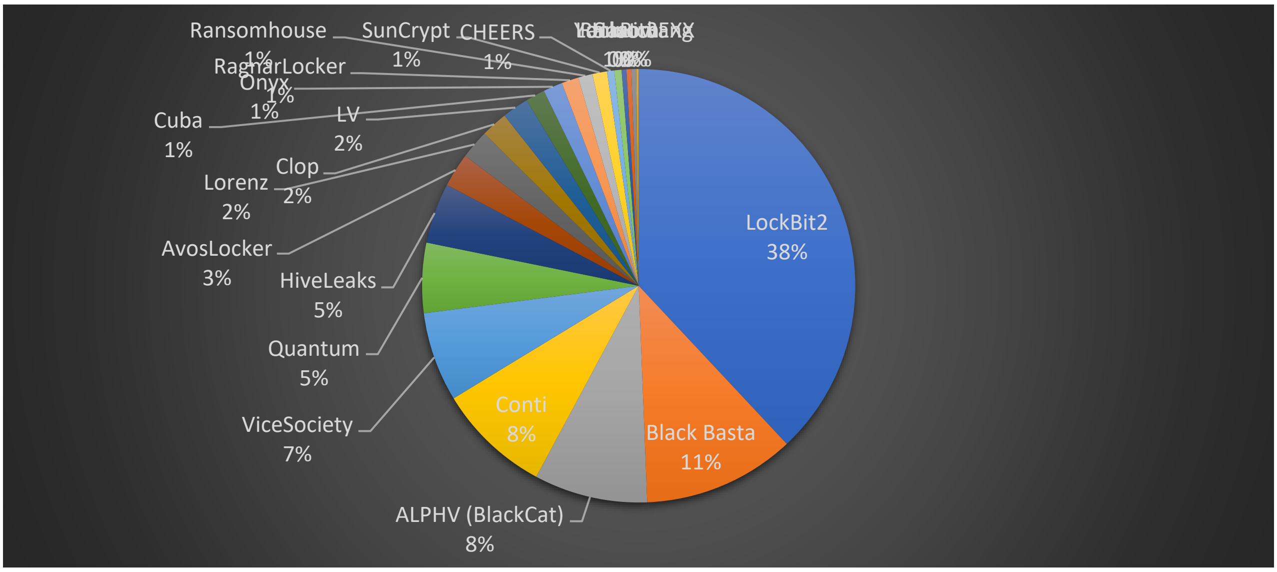


Cyber Extortion groups activity Q1 to Q2 2022

Victimology of Q2 2022

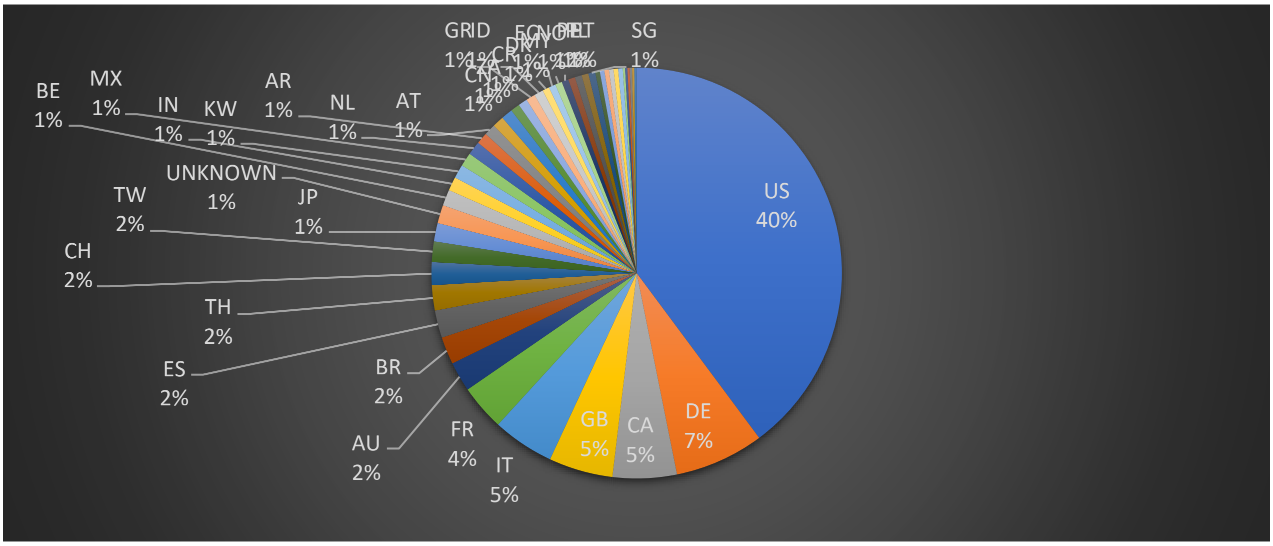
Q2 2022 has shown very similar numbers of victims being extorted on the so-called leak sites on the dark web. While we have observed major changes in threat actor distribution, we see that other threat actor groups are picking up the ‘share’ and thus we only registered a 2% decrease of extorted businesses in comparison to the previous quarter. During Q2, LockBit2 remained the top actor causing the highest victim count of 211 (a share of 38%), followed by Black Basta with 63 victims (11%). This is a new observation since Conti has been taking the spot of the second most active threat actor over the past months, except for May and June 2022 when they started to cease operations.

The third most active threat actor in Q2 was ALPHV, also referenced to as BlackCat. This actor has leaked 47 victims coming from industries such as Professional Services, Manufacturing, Educational Services, Finance and Insurance as well as Utilities.



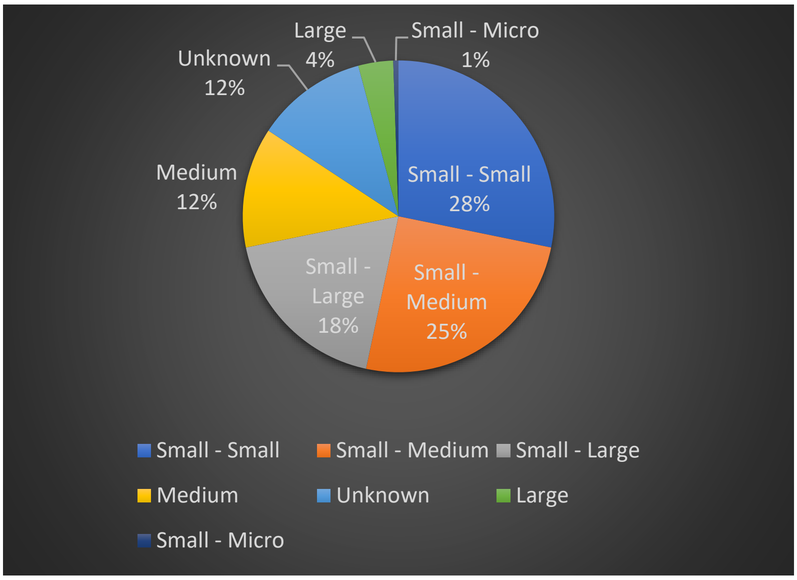
Contributors to cyber extortion leaks in Q2 2022

The countries that have been most impacted by this threat are the U.S., with 221 victim businesses, Germany (39 victims), Canada (28 victims), United Kingdom (28 victims) and Italy with 27 victims in Q2 2022. Brazil, Spain, Thailand, China and Taiwan are also represented in the top 10 impacted countries. This trend is fairly new and entails that we see less growth in U.S.-based businesses and a much faster growth in regions such as East Asia (CN, JP, KR, TW, HK, MN), the Middle East (BH, JO, KW, QA, SA, SY, TR, AE, LB, OM), the Nordic countries (DK, FI, NO, SE), Southeast Asia (ID, MY, VN, SG, TH, PH) and Latin America (BR, MX, AR, CO, CR, DO, PE, PR, CL, BO, EC, VE, HN, PA, PY, NI, GT).



Victim organization's country in Q2 2022

Businesses most impacted by cyber extortion in Q2 were small organizations with an employee count varying from 1 to 999 (as can be seen below), accounting for almost 3/4 of all victims (n=406). Mediumsized businesses represented 12% of victims (n=69), and 20 businesses victimized with an employee count over 10,000 were registered during Q2 (4%). These large businesses originated from the Manufacturing sector (n=8), Retail (n=6), Professional Services (n=2), Agriculture, Forestry, Fishing and Hunting (n=1) and Healthcare (n=1). The top three threat actor groups that compromised large organizations were Black Basta, LockBit2 and Ransomhouse.



Size of businesses impacted by cyber extortion in Q2 2022

Business size classification

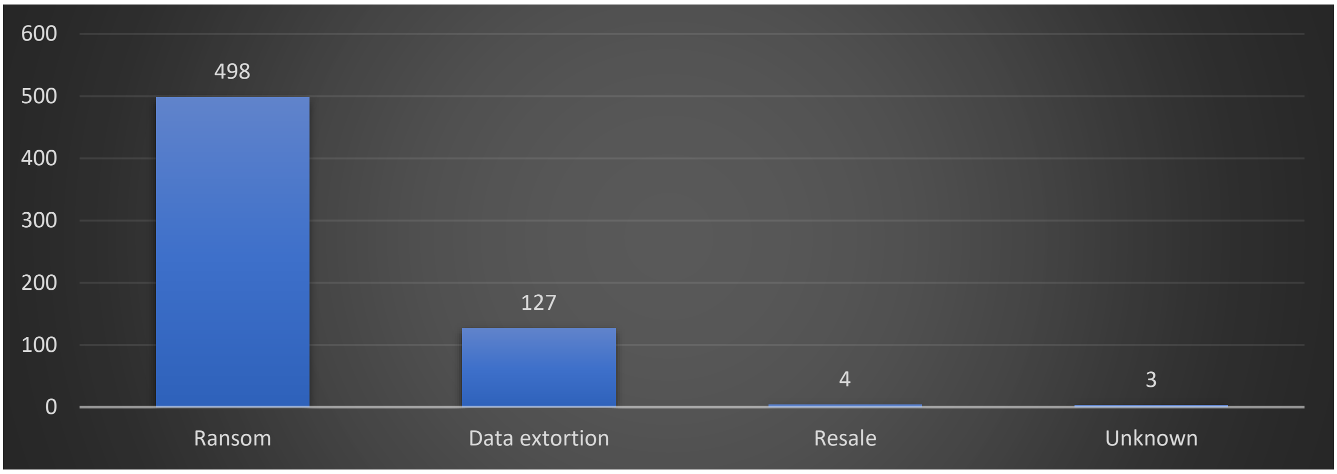
Small – Micro: 1-9 employees
Small – Small: 10-49 employees
Small – Medium: 50-249 employees
Small – Large: 250-999 employees

Medium: 1000-9,999

Large: 10,000+

And lastly, as we have argued previously, the current threat we are observing needs to be called cyber extortion instead of ransomware. The reason for this is that we don’t necessarily see attacks that encrypt the victim’s files and systems. We sometimes observe threat actor groups openly declaring that they do not see the need for encryption any longer. Instead, they apply other extortion techniques. One of them is data exfiltration, which is used to extort money from the victim organizations. During Q2, we have observed several new threat actor groups that do not encrypt but ‘data extort’ only. When we find out that a threat actor is operating with data extortion only, we register this in our documentation and classify the attack type for these groups as ‘Data extortion’ instead of ‘Ransom’.

In Q2, we saw the majority of victims still suffering a ransomware attack (79%) with additional extortion techniques such as threatening to resell or publish the stolen data on top of demanding payment for the decryption key. Additionally, we observed that 20% of attacks used data extortion only to coerce money from the victim organizations. One percent were threatened by selling the victim’s data and three cyber extortion attack types remained unknown to us.



Attack Type applied during Q2 2022

Editor's Notes (Beta)

This section is relatively new and was introduced in the January 2022 monthly report. 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.

Charl

Mobile device threat and Apple's response

https://www.orangecyberdefense.com/global/security-navigator

In our 2022 Security Navigator report we made some comments on what we consider to be the emerging threat of attacks against mobile devices, and specifically Apple iOS. I'm going to quote that opinion almost verbatim here, before commenting in a recent update to this theme…

Security Navigator 2022:

Back in 2019, we posited that as more systems enforced Multi Factor Authentication using mobile phones, mobile phones themselves would become increasingly targeted by attackers wanting to subvert the authentication process. We started tracking this development via our World Watch advisories, looking for evidence of this as a reality. Before the first quarter of 2020, we never saw any.

In the third quarter of 2020, however, we started seeing a wave of vulnerabilities and attacks against mobile phones, and especially Apple iPhones, by commercial companies contracted to government law enforcement and intelligence agencies. These attacks appear designed to compromise the phones of specific 'high-value' persons of interest. They require extraordinary investment, skilled people and zero-day exploits.

Attacks are conducted against specific targets using commercially developed toolkits that are used to compromise and track individuals' phones. The actual compromise often requires special 'zero-day' exploits, which are not always developed by the toolkit vendor itself.

Exploits are often bought on an open market and often provided by brokers who facilitate transactions between private exploit developers and commercial 'Offensive Cyber Technology' vendors. The value of such exploits is extraordinary. Corporate security budgets pale in comparison to the sums of money that flow through government 'national security' budgets via vendors and brokers to black market exploit developers.

Exploit broker Zerodium is currently offering up to $2 million for an iOS exploit.

Offensive Cyber Technology vendors sell primarily to governments, at extraordinary prices. But such companies also emerge within government agencies. This creates a kind of cycle known as the 'Cyber Military Complex'.

Thus, we see there is a repeating pattern of demand and supply that fuels the creation of new capabilities and extraordinary spending. This money, the skills, experience and resulting capabilities do not stay in the government domain, however. History has shown that there is a constant process of osmosis via which exploits, toolkits, training, skills and experience 'bleed' from the government, military, and intelligence domains into the cybercrime ecosystem, where they impact directly on civilian businesses and their customers.

A fundamental systemic driver for the challenges we face in information security is therefore the convergence of government spending on hacking technology and criminal innovation, which greatly 'inflates' the security challenge. This convergence, fueled by extraordinary levels of government investment, can completely invert the risk 'calculus' most businesses use to determine their security strategies.

It is thus noteworthy that this dynamic has recently been most visibly demonstrated in vulnerabilities and attacks against mobile phones, and particularly Apple's iOS.

Due to their high cost and highly targeted nature, iOS exploits have not caused our typical customers much concern in the past, and mobile security has not traditionally been a very high priority for businesses. That may be starting to change.

In March 2021, Microsoft announced that 'passwordless' sign-in was 'generally available' for commercial users, bringing the feature to enterprise organizations around the world. Microsoft clients 'can now completely remove the password from your Microsoft account. Use the Microsoft Authenticator app, Windows Hello, a security key, or a verification code sent to your phone or email to sign into your favorite apps and services, such as Microsoft Outlook, Microsoft OneDrive, Microsoft Family Safety, and more'.

There appears to be little doubt that other cloud services providers, as well as Identity Service Providers, will soon follow suit. And this is an exciting net gain for security. It does, however, signify a systemic shift for the threat landscape, as a 'passwordless' future often involves the users' mobile phones as a core component of the corporate security 'perimeter'.

We anticipate that three systemic factors are likely to converge soon:

1. Government spending on mobile phone hacking will fuel a continued growth in these kinds of hacking capabilities, which will not remain confined to the cyber military complex.

2. More vendors will (thankfully) adopt a 'passwordless' paradigm.

3. This will result in a shifting focus to the role of the mobile phone as a key component of the security perimeter security stack.

This suggests that patching and monitoring of user mobile phones will become increasingly important as our reliance on passwords for authentication finally starts to wane.

July 6, 2022: Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware:

https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

On July 6th Apple announced that it was “previewing a groundbreaking security capability that offers specialized additional protection to users who may be at risk of highly targeted cyberattacks from private companies developing state-sponsored mercenary spyware”. Apple also published details of its “$10 million grant to bolster research exposing such threats”.

The new set of security features is being labelled ‘Lockdown Mode’, and it should be available in Autumn 2022 with iOS 16, iPadOS 16, and MacOS Ventura.

At launch, Lockdown Mode includes the following protections:

- Messages: Most message attachment types other than images are blocked. Some features, like link previews, are disabled.
- Web browsing: Certain complex web technologies, like just-in-time (JIT) JavaScript compilation, are disabled unless the user excludes a trusted site from Lockdown Mode.
- Apple services: Incoming invitations and service requests, including FaceTime calls, are blocked if the user has not previously sent the initiator a call or request.
- Wired connections with a computer or accessory are blocked when iPhone is locked.
- Configuration profiles cannot be installed, and the device cannot enroll into mobile device management (MDM), while Lockdown Mode is turned on.

Apple is positioning this excellent set of features as being aimed toward a ‘small set of users’ who face extraordinary threats. This is a welcome and necessary step on their part, and initiative we hope other vendors will seek to emulate.

But we differ with Apple that this effort is only relevant to a select group of extraordinary individuals. As we outlined in our Security Navigator report, we believe that the stage has been set for a dramatic increase in attacks against business user mobile devices, at least in part by criminals seeking to subvert Multi Factor Authentication processes that rely on mobile phones. In our view, today’s “high risk individual” is tomorrow’s “regular corporate user”. In other words, while these features may be considered excessive and restrictive in today’s corporate threat landscape, we anticipate that this will not be the case in near future.

We welcome this early effort by Apple, not only to address the threat to today’s vulnerable individuals, but also to lay the groundwork for a more robust and comprehensive toolkit with which our customers can counter the threats of tomorrow.

Wicus

The need to verify

In early 2018 the world learned about side channel vulnerabilities called Spectre and Meltdown in CPUs manufactured by Intel, AMD, and others. The irony of these side channel vulnerabilities is that these were unwittingly introduced to improve performance through a clever technique that helps the CPU predict which execution path a piece of code could take. If the prediction was correct then the additional work was worth it, but if it was wrong in its prediction then nothing was lost because the CPU did these extra computational cycles in the background anyway.

Other clever folks in lab coats figured out that it is possible to leak information by making the CPU do work on memory that is technically off-limits under normal execution conditions by tricking the branch prediction features to run ahead and read the confidential memory before the CPU realized its mistake. Intel, AMD, and others with the help of operating system developers created mitigations that prevented these types of side channel attacks.

New research by ETH Zurich has shown that mitigations known as ‘retpoline’ are not effective. These researchers proved they can leak a Linux operating system’s root password in about 28 minutes when running on Intel Skylake-based CPUs, and about 6 minutes when running on AMD ZEN, ZEN+, and ZEN2 CPUs.

Both Intel and AMD recommend that the Indirect Branch Restricted Speculation (IBRS) be implemented. The documentation published by AMD and Intel would suggest that Windows already have this mitigation enabled by default, while the Linux kernel and some hypervisors rely on the retpoline mitigation instead. IBRS is being made available to the affected operating systems to mitigate the new vulnerability named ‘Retbleed’. These mitigations will introduce performance loss of anything from between 12 to 28 percent depending on the vendor and workload.

The research to determine if the fix is effective, especially for such a peculiar class for a vulnerability, is invaluable. It is not just anyone that can perform this type of research due to its very technical and specialized nature. The fact that someone was able to dedicate time and resources to this in itself is amazing. I wonder if the news cycle would have published any content if the researchers confirmed the effectiveness of retpoline instead.

Reproducing research or testing claims is something you seldom hear about. It must be human nature to gravitate to the novel and new rather than rehash something familiar. People tend to pay little attention to the result unless it is contrary or controversial. Thus, the perceived waste of time or rejection by others may deject most researchers to revisit existing work. There could also be an underlying social barrier that cause people to stay away from questioning someone’s work that has been accepted by the masses.

The difficulty with most of the vulnerabilities that are discovered and fixed seems to be that the average person must blindly accept that these are fixed adequately. Similarly, we must accept that the software or hardware we use have yet to be discovered vulnerabilities, but we do not have the ability to do anything about it until it is revealed. The reality is the more we become dependent on technology the greater the overhead becomes to manage the inherant risk. It seems that reducing risks involves a fine balance to limit exposure to certain kinds of technology, even possibly eliminating certain things all together.

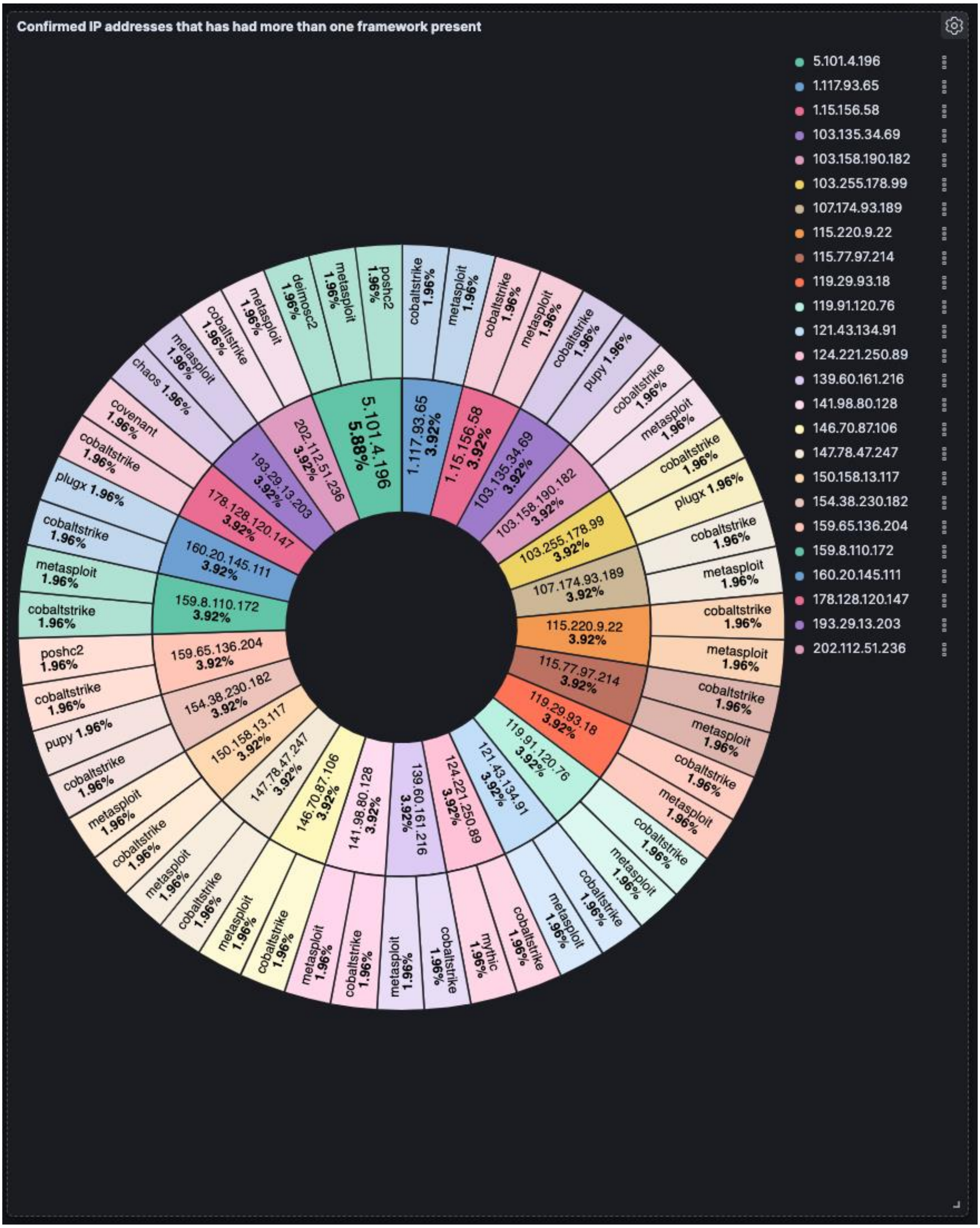
Tales from the Trenches (Beta)

Our Tales from the Trenches for Q2 2022 comes in the form of an update from our newly formed Advanced Intelligence & Detections team who are based out of Malmo. This update focuses on the work they are doing to track post exploitation frameworks and other malware.

The **Advanced Intelligence & Detections** (AID) are focusing on only two things: Detection Engineering and Operational Threat Intelligence.

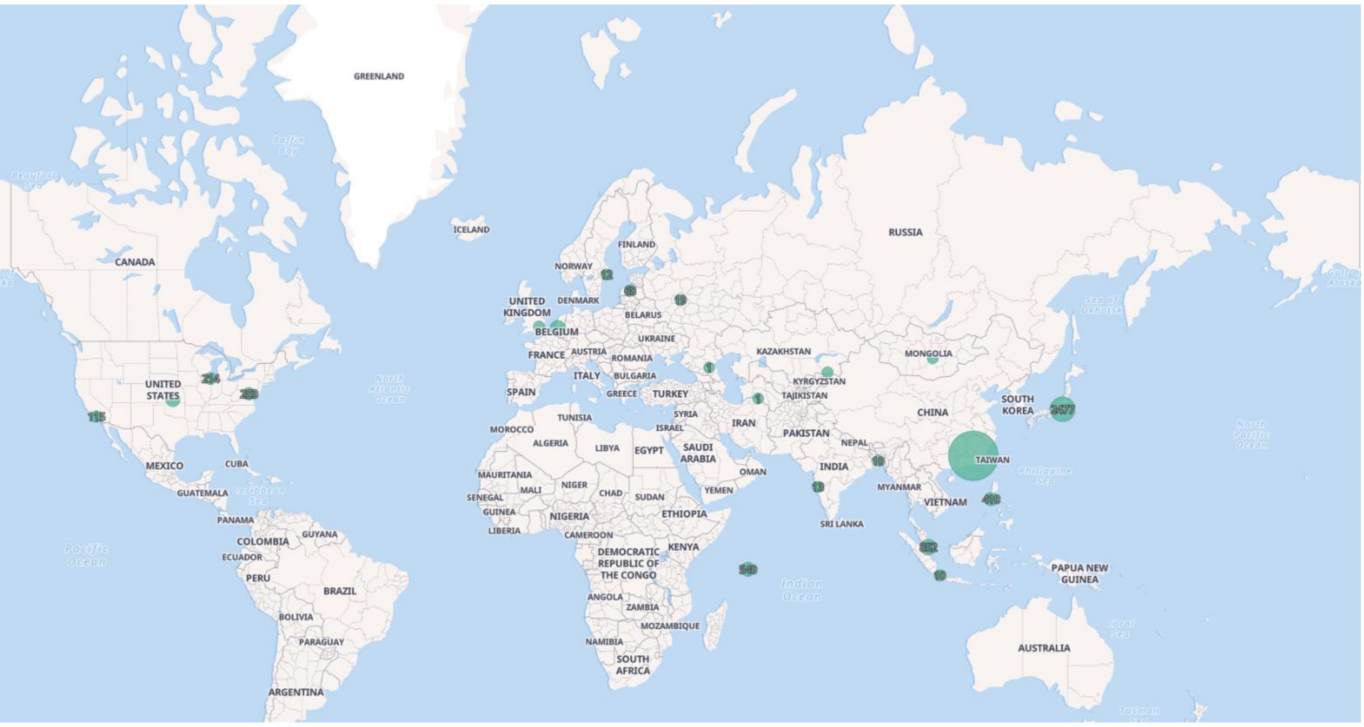
Peerpressure is (if you are unaware) the system we have engineered to speak with C2 infrastructure on the internet and then automatically pass information on confirmed destinations to our customers. It means that we develop individual probes that “speak” the same language as the different tools. We started more than a year ago with Cobalt Strike but it has now expanded way beyond that.

This first illustration is pretty cool. We can now track IP addresses with ports over time and see if anything has hosted more than one framework. We find this interesting to learn about what tools are commonly combined since most often it is the same threat actor over time that reuses the same IP.



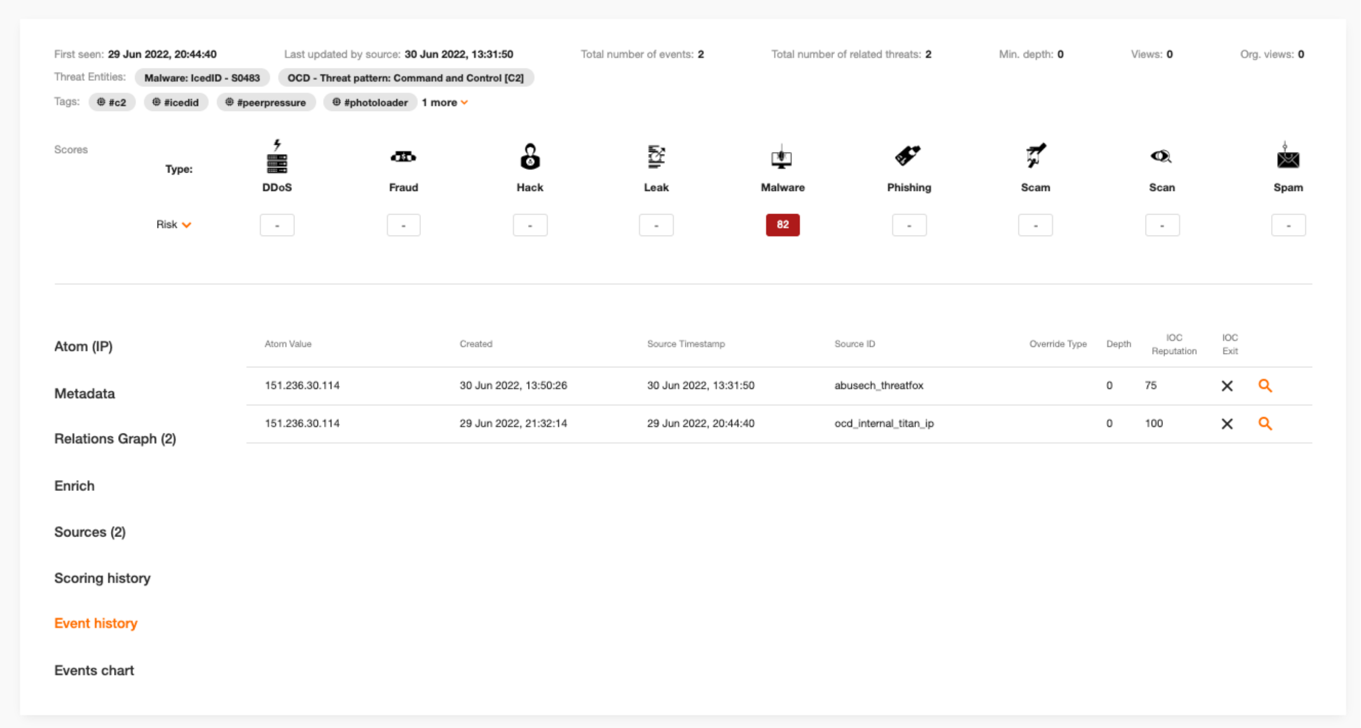
Confirmed IP addresses that has had more than one framework present

We are doing a bit of improvements on geolocation data and although this is not 100% the world map of PlugX is pretty interesting. Commonly a tool used by APT10, APT41 and other Chinese threat actors the hotspots are also located in Asia.



Not only do we do post exploitation frameworks we also track IcedID and Qakbot today. Below is a screenshot from one of our internal tools called the Datalake and this is where we gather threat intelligence. It will report timestamps when someone reports in something bad, in the example below the label “ocd_internal_titan_ip” refer to a detection we contributed. In this case it is some hours before a third-party called Abuse.ch.

The good thing about this is that we are talking the same “language” as both IcedID and Qakbot so it means we can retrieve archived communication to respond to queries about true positives or false positives.



First seen: **29 Jun 2022, 20:44:40** Last updated by source: **30 Jun 2022, 13:31:50** Total number of events: **2** Total number of related threats: **2** Min. depth: **0** Views: **0** Org. views: **0**

Threat Entities: **Malware: IcedID - S0483** **OCD - Threat pattern: Command and Control [C2]**

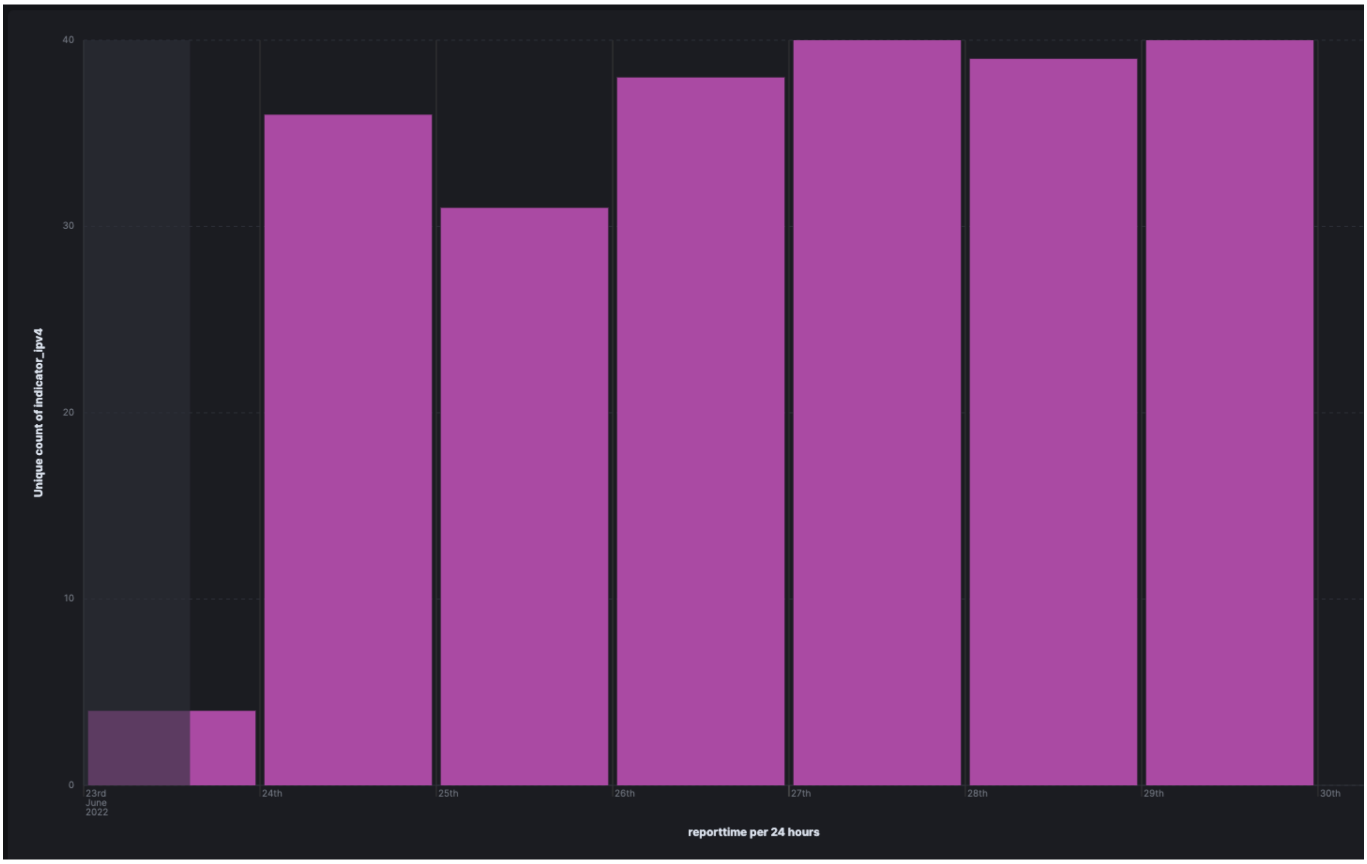
Tags: **#c2** **#icedid** **#peerpressure** **#photoloader** **1 more**

Scores

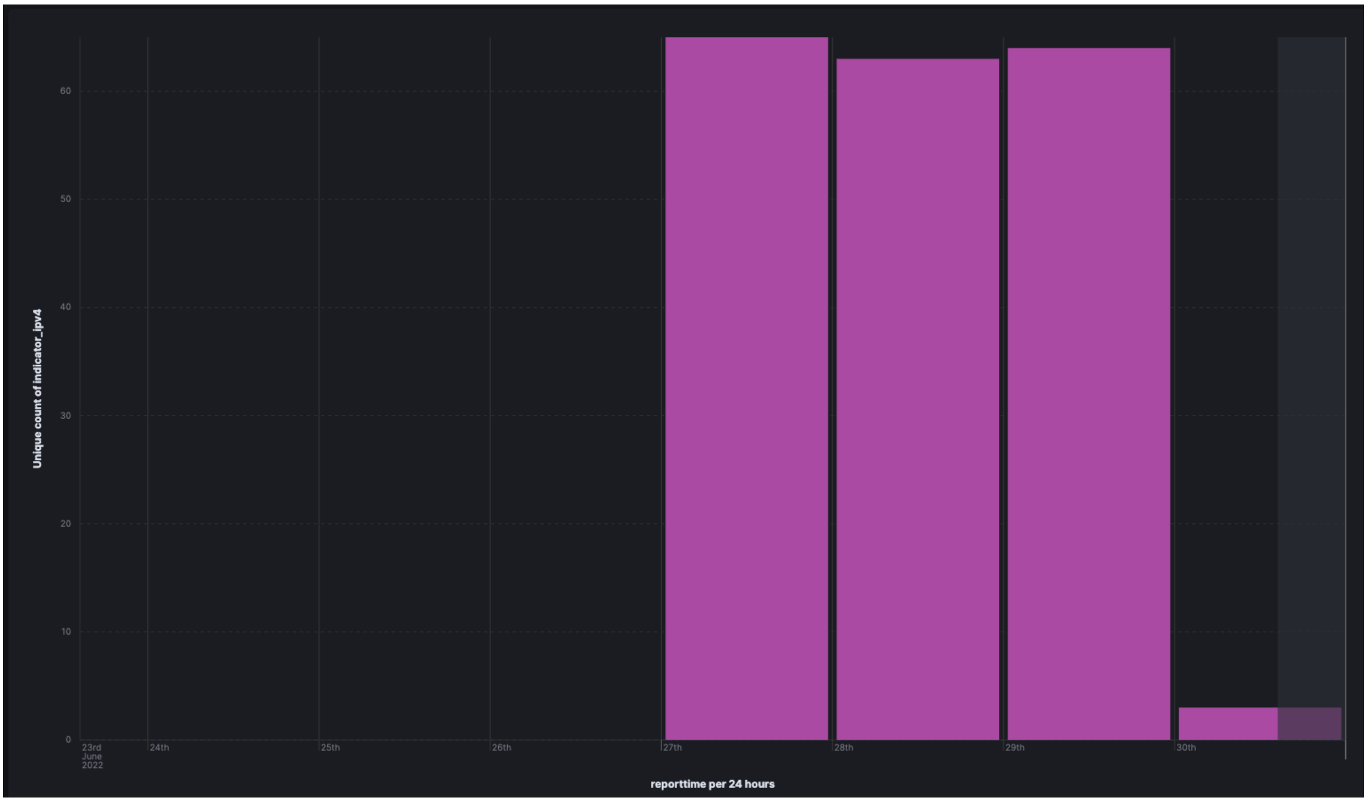
Type:	DDoS	Fraud	Hack	Leak	Malware	Phishing	Scam	Scan	Spam
Risk	-	-	-	-	82	-	-	-	-

Atom Value	Created	Source Timestamp	Source ID	Override Type	Depth	IOC Reputation	IOC Exit	
151.236.30.114	30 Jun 2022, 13:50:26	30 Jun 2022, 13:31:50	abusech_threatfox		0	75	✕	🔍
151.236.30.114	29 Jun 2022, 21:32:14	29 Jun 2022, 20:44:40	ocd_internal_titan_ip		0	100	✕	🔍

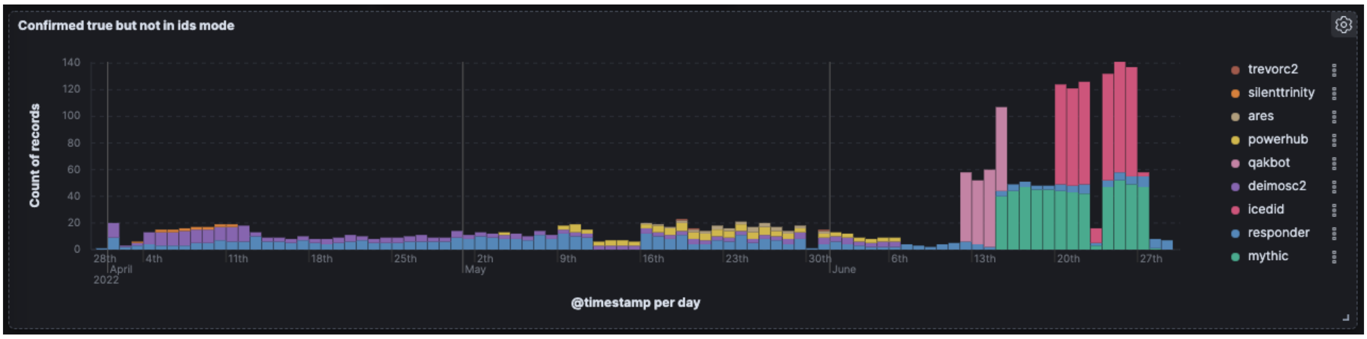
In the example of Qakbot we confirm about 40 C2 servers on a daily basis. So, we assume that this is the total C2 infrastructure size at any given point in time.



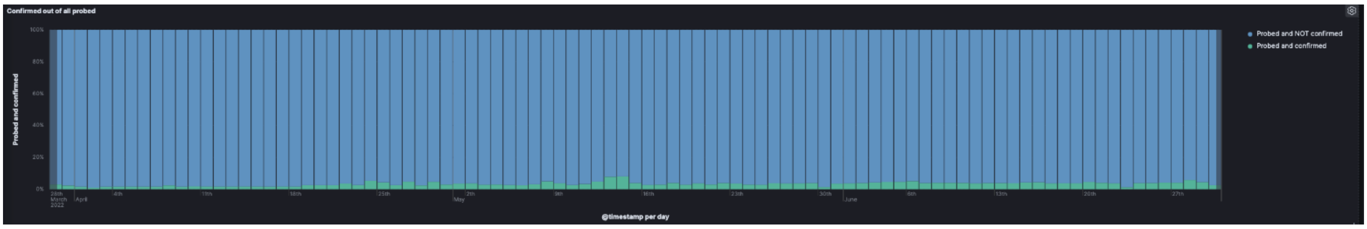
The latest addition, IcedID, is a bit bigger when compared with Qakbot. Here we can see above 60 C2 servers almost every day so far.



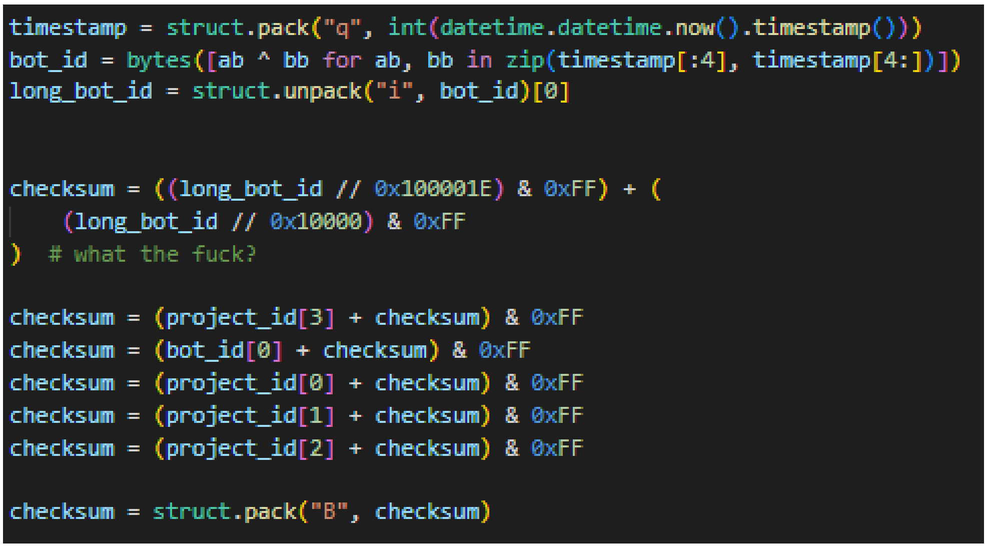
Here is a graph that shows a bit of the stuff that has been in the works and what is constantly released. Basically "ids mode" means that we release it into production, so customers get access to the data. Below you can see the different families we have in "pre-production" over the last months. This shows a bit of stuff that is in the backlog but also that we are quite busy working on new things. Here you can see the amount of days roughly we let things run before we think we are good enough and got it all figured out.



On the topic of how we measure performance we can see below that a great deal of endpoints we identify we are not able to confirm. This really shows the value of how it works. That we are quite broad at the things we gather and the end results is very accurate. We can also see that we keep the same performance over time.



The screenshot below is from a team member that is working on improvements the IcedID prober. More specifically how to construct the right checksums to "speak" IcedID properly. This is inspired by https://en.wikipedia.org/wiki/Fast_inverse_square_root



```
timestamp = struct.pack("q", int(datetime.datetime.now().timestamp()))
bot_id = bytes([ab ^ bb for ab, bb in zip(timestamp[:4], timestamp[4:])])
long_bot_id = struct.unpack("i", bot_id)[0]


checksum = ((long_bot_id // 0x100001E) & 0xFF) + (
    (long_bot_id // 0x10000) & 0xFF
)  # what the fuck?

checksum = (project_id[3] + checksum) & 0xFF
checksum = (bot_id[0] + checksum) & 0xFF
checksum = (project_id[0] + checksum) & 0xFF
checksum = (project_id[1] + checksum) & 0xFF
checksum = (project_id[2] + checksum) & 0xFF

checksum = struct.pack("B", checksum)
```

We will continue to work as usual during the next couple of months while the northern hemisphere is enjoying summer and since the backlog contains about 100 different frameworks and malware families we think we will be busy for the foreseeable future.

Good News Cyber

Law enforcement success starts off our good news cyber section again this month. In this instance an operation, codenamed "First Light 2022", led to the seizure of 50 million dollars and the arrests of thousands of people involved in social engineering scams worldwide.

Interpol led the operation, with the assistance of police from 76 countries, which focused on various social engineering crimes including business email compromise (BEC) scams, telephone deception, romance scams, and the money laundering activities associated with these.

The First Light 2022 operation ran between March and May 2022, and had the following results:

- 1,770 locations raided worldwide
- Some 3,000 suspects identified
- Around 2,000 operators, fraudsters, and money launderers arrested
- Some 4,000 bank accounts frozen
- In the region of USD 50 million worth of illicit funds intercepted

Away from law enforcement we have seen decryptors released for two separate ransomware variants. Firstly, the Korea Internet & Security Agency (KISA) published a decryption tool, along with usage instructions, for the Hive ransomware variant. The second one came from Avast following an analysis of the Harditem variant, which they discovered to be a decryptable variant of Prometheus/Thanos, their existing decryptor was updated to include this variant.

Sticking with ransomware, the threat actors behind the not so well known AstraLocker ransomware variant announced they were shutting down their operations and were intending to make a shift towards cryptojacking instead. The developer of the ransomware uploaded a zip file to the VirusTotal platform containing a number of AstraLocker decryptors, one of the decryptors was tested by Bleeping Computer and confirmed as working. It was reported that Emsisoft are now currently working on a universal decryptor for AstraLocker.

Finally, as covered earlier in this report, Apple has announced that they will be introducing "Lockdown Mode" in iPadOS/iOS16 and Mac OS Ventura. Whilst the aim of this is to considerably improve a device's security posture by disabling features to reduce the attack surface, this will also have an impact on the usability of the device. Apple are positioning “Lockdown Mode” as being aimed toward a ‘small set of users’ who face extraordinary threats, meaning those individuals will have to make the choice between the security of their device and its usability/features.

Verizon Data Breach Investigations Report 2022 Overview

Summary

The Verizon Data Breach Incident Report for 2022 can be summarized with “Ransomware is everywhere” and “Business Email Compromise is lurking in your inbox”. Cybercrime is an escalating problem while incidents or breaches related to Espionage, Ideology or Grudge are also present in DBIR 2022, but these are in the minority compared to financially motivated breaches or incidents.

The use of stolen credentials is a constant theme in the DBIR. Attacker are taking the easy road and use credentials to log into systems remotely or gain access to email accounts. Social engineering through phishing and pretexting is big enabler to steal credentials or get victims to open the door to further attacks. Phishing is a favorite to get direct access to an organization by delivering malware through malicious office document attachments. It is 2022, but these techniques still work better than ever.

Credentials and Personal Identifiable Information (PII) are highly sought-after data types and feature most prominently in the DBIR. Breaches involving medical records and payment card information feature, but much less so compared to PII. Payment card information and health care information have received much more rigorous scrutiny over the past decade and many businesses with this type of data have made considerable investment to guard these. Strong privacy and protection regulations have not been in place for as long as PCI DSS for example.

The single biggest lesson from DBIR 2022 is to mandate multi-factor authentication (MFA) for all accounts that can access services from the Internet. The report does not explicitly mention any MFA approach, but we recommend phishing resistant hardware authentication tokens that are FIDO2 certified. These kinds of tokens must be used with administrative accounts to provide strong additional protection for these sensitive accounts. Normal staff accounts must also be protected using MFA. We recommend using current model mobile phones with authenticator apps that are paired with an industry recognized Single Sign On service.

The lack of suitable endpoint protection or anti-virus solutions ensure that malware can easily be deployed throughout the organization. Defending the endpoint is a first step to guard against ransomware.

Deeper dive

The Verizon Data Breach Investigation Report (DBIR) 2022 celebrates its Fifteenth year and was first published in 2008. Over these fifteen years the DBIR team examined 914,547 incidents and 234,638 breaches.

The DBIR 2022 report includes 23,896 security incidents and 5,2122 breaches. An incident is defined as a security event that resulted the violation of a business asset’s Confidentiality, Integrity, or Availability. A breach is an incident in which there was a confirmed disclosure of data by an unauthorized party.

The Verizon DBIR team has additional requirements when deciding to include a security incident in the caseload to ensure that the data set quality is good. To do so requires a brief explanation of the Vocabulary for Event Record and Incident Sharing or VERIS framework. VERIS is a methodology that is used to annotate an incident or breach by using several data points of interest. All incidents in the DBIR are mapped to VERIS to ensure consistency in the way an incident or breach is analyzed and classified.

Coming back to the qualifiers to include incidents in the DBIR data set. An incident must have at least seven VERIS enumerations across 34 possible fields or be classified as a Distributed Denial of Service

(DDoS) attack. Confirmed data breaches are treated as an exception even if it has less than seven enumerations. Additionally, the incident must have at least one known VERIS threat action category, for example malware, hacking, social, etc. All incidents must be linked to a business and incidents involving individuals are not considered. The incident must also have occurred during November 1, 2020, and October 31, 2021. This is referred to as the 2021 caseload.

Verizon received several data set contribution from partners spanning the globe to the 2021 caseload. The DBIR team had to qualify each contribution based on the criteria mentioned above.

The DBIR data is non-exclusive multinomial. This means that a single feature can have multiple values and this in turn means that all percentages does not necessarily add up to 100%.

Ransomware, unfortunately, is very present in the data set. Ransomware has grown to represent 25% of all breaches from 2017 to 2021, compared with 12% in 2020. The report also states that the four key vectors for a breach, excluding error and misuse, are use of stolen credentials, phishing, exploiting vulnerability, and botnets. Blocking these four paths would certainly cut the number of ransomware cases dramatically. These four areas are prevalent throughout the DBIR report and indicates that businesses must have plan to address these attack varieties.

Partner or supply chain related breaches account for sixty two percent of all breaches that involved System Intrusion. System Intrusion involves lateral movement and an attacker can use various techniques to access parts of the system. This type of action is normally considered more complex and can involve actions such as user manipulation (Social), Hacking and Malware. Knock on effects from incidents that impacted SolarWinds, Kaseya, and Accellion spilled over into this part of the DBIR 2022. Other supply chain incidents not involving these vendors were also included in this caseload.

Approximately 90% of incidents involved hacking of servers. The bulk of this consist of Internet exposed web servers (56%) or email servers (28%). The ProxyLogon set of vulnerabilities in Microsoft Exchange server did not help here either. Email servers have also been targeted as part of Business Email Compromise (BEC) attacks and did not necessary involve exploits, but something simpler namely the Use of Stolen Credentials.

Personal Identifiable Information (PII) and credentials remain the most sought-after data variety. Payment data has since 2018 remained relatively flat and below 15% for breaches, compared with Personal Identifiable Information (+-50%) and credentials (+-45%). Looking back to the DBIR of 2008 we saw Payment Card Data was at 84% and PII was at 32% for all breaches. The authors make the statement that Payment Card Data is much more difficult to get hold of, but PII is so much more readily available and in demand.

We can see that Ransomware related activity (Obscuration) is the leading cause where Availability is impacted sitting at over 80% for this class. Only 38% of breaches involving Ransomware saw Confidentiality being impacted. This is strange when one considers the prevalence of Ransomware leak sites.

'Actor Disclosure' ranks at more than 50% as the number one breach discovery method. This is no surprise that ransomware or the listing of victim's data on a criminal forum is sighted as the factors contributing to this. In other words, victims find out of the breach because the attacker made the victim aware of the breach explicitly.

The DBIR report also lists the number of steps taken by an actor in a breach, excluding breaches involving error. According to the report the most actors require between two and five steps to be success in breaching the victim. Phishing, Downloader (malware), and Ransomware are the three most common steps in such a breach. Long attack chains are likely to be thwarted and yield less results whereas shorter attack chains are effective.

Denial of Service features rather prominent in the Incident Patterns variety and this include the network layer, for example Distributed Denial of Service, and the application layer with website defacement being at the bottom end. Hand in hand with this is Basic Web Application Attacks, followed by System Intrusions. Social Engineering remains a prominent attack pattern. Lost and Stolen Assets, Miscellaneous Errors, Privilege Misuse, and everything else being the least likely attack pattern for incidents.

A leading Breach Pattern is System Intrusion, followed by Basic Web Application Attacks, and Social Engineering. Once again Ransomware is to blame here. This claim is backed by the fact that 93% of all breaches with this pattern is motivated financially and only 6% is ascribed to Espionage. Partner or Supply Chain incidents are represent 60% of the attack vectors related to System Intrusion, matched by (malicious) Software Updates. The report insinuates that this could be linked to the SolarWinds incident. What is also interesting to note is that the System Intrusion is also made possible by targeting Desktop sharing software such as Microsoft Remoted Desktop (RDP) and email. The data also mentions that “office doc” file types are the leading cause for malware infection delivered using email.

One would think that phishing is the main cause of ransomware infections, but the DBIR report shows that the use of stolen credentials combined with desktop sharing software is in fact the number one path of ransomware. Email and phishing as a vector occupy the second spot, while exploiting web application vulnerabilities occupying the third position on the podium.

The role that vulnerabilities play in leading to a breach or incident is something to ponder. Exploitation of vulnerabilities is up to 7% of breaches in 2021. This is a twofold increase over 2020. How do attackers go about identifying these vulnerabilities and is this targeted or opportunistic? The DBIR makes an argument that points more to the latter. The report goes as far to show that attackers are pragmatic in their approach by scanning IP addresses and ports for specific services. Next, they crawl or explore these discovered hosts and services, finally test for known vulnerabilities. The DBIR shows that single use remote code execution vulnerabilities are discovered 0.4% of the time. In the data set this is present 4,740 times.

The report also shows that businesses are getting better at patching their systems in response to an incident. Ninety percent of businesses address issues related to an incident within the first seven days compared with less than 75 percent of businesses being able to do so for the same period in 2020. The 2021 report also shows that victims address 100% of the issues related to an incident within 90 days. Compare this to 2020 and 2019 that took longer than 90 days.

People were involved in 82% of breaches during 2021. Social Engineering is in many cases the first step of a breach. The top three action varieties, or attack paths, consist of phishing (+-75%), use of stolen credentials (+-35%), and pretexting (+-27%). Pretexting requires considerably more work and involves the attacker contacting the victims directly. The follow on or secondary step for most Social Engineering attacks is either malware being deployed, or credentials being stolen. The report also highlights that pretexting is mainly associated with Business Email Compromise (BEC) in this data set. Only 41% of BEC incidents involved phishing. Looking at the remaining 59%, we see that of that 43% involved the use of stolen credentials. The remainder use compromised partner email accounts or other email accounts.

Basic Web Application Attacks (BWAA) targets Internet-exposed web and email services. Breaches involving this attack mainly involves the use of stolen credentials to access a business’ assets. Types of data compromised are Personal, Credentials, Medical and other. The motives of the actors are mainly financial gain (65%), but espionage (31%) also features high. Grudge (2%) and hacktivism or ideology (1%) also features. Surprisingly enough 20% of espionage cases leverage BWAA and are attributed to state affiliated attackers.

Miscellaneous Errors by definition can only involve internal staff. Breaches in this class is perpetuated through Misdelivery or Misconfiguration. Types of data disclosed include PII (81%), Other (23%), Medical (18%), and Bank details (8%). Top exposed assets are email servers, database servers, documents, and other.

Denial of Service, on the other hand, is executed exclusively by eternal actors. This type of attack is very common and the DBIR recorded 8,456 incidents. By now there are tried and tested means to deal with this kind of incident and business must include mitigations for this type of attack. The median Distributed Denial of Service DDoS attack reached 1.4 Gbps, with some reaching more than 99 Gbps. Fifty percent of recorded DDoS attacks lasted less than 4 hours. One percent of companies experienced more than 1,000 DDoS attacks per annum, while the majority observed less than 10 DDoS attacks per year. The top three industries that were on the receiving end of DDoS attacks were Professional Services, Information Services, and Manufacturing.

In most cases incidents involving lost or stolen assets are considered incidents as there is no way to know if data was disclosed for certain. In contrast where theft is involved the data is considered disclosed and handled as a breach. Such breaches involve the theft of user devices such laptops, desktops, mobile phones, or other media such as paper documents. The majority (98%) of these thefts are motivated by financial gain, while a small portion (2%) are attributed to ideology.

Privilege Misuse, like Miscellaneous Errors, is attributed in large (100%) to internal actors such as staff, with external actors (4%) in combination with staff (4%) colluding or unknowingly helping the other. Main motivators for these breaches are financial (78%), followed by grudge (9%), espionage (8%), and convenience (6%). The latter, convenience, occurs when staff break rules or abuse privileges to sidestep controls that make their job more difficult resulting in data mishandling. Businesses need to educate their staff as to why certain controls are important, but also design controls to be as frictionless as possible.

The DBIR use the North American Industry Classification System or NAICS to classify businesses according to industry. The DBIR divide businesses into small, 1 to 1000 employees, and large, more than 1000 employees. Most businesses in the data set were not classified per business size and almost a fifth of businesses could not be assigned an industry classification.

The most common breach pattern is System Intrusion. Hacking and Malware were the most prevalent breach action. The Server asset class featured prominently for breach asset classes. These three breach attributes play well into the ransomware narrative. Following on the heels are targeting of Persons using Social Engineering. Looking at incidents, in other words security events that did not lead to data disclosures, we see a repeat of what was observed with breaches. The only difference is that Denial of Service is now more prominent.

The top six featured industries with the highest number of incidents are Professional Services (3,566), followed by Public Administration (2,792), Information (2,561), Finance and Insurance (2,527), Manufacturing (2,337), and Education (1,241). Healthcare (849) and Retail (629) did not make four figures. Of the 23,896 incidents, only 2,065 incidents were associated with small businesses and 636 incidents were associated with large businesses. There reset are unclassified. Proportionally this matches what the Orange Cyberdefense Secure Research Centre has seen with victims in the Cyber Extortion data. Businesses smaller than 1001 employees tend to feature more in incidents and breaches. The reason for this could be as simple as there are more smaller businesses than large businesses. Also, larger businesses can employ dedicated professionals to look after security and infrastructure, thus managing their risk better.

The DBIR drilled into 11 industries. These are:

- Accommodation and Food Services (NAICS 72)

- Arts, Entertainment and Reaction (NAICS 71)
- Educational Services (NAICS 61)
- Financial and Insurance (NAICS 52)
- Healthcare (NAICS 62)
- Information (NAICS 51)
- Manufacturing (NAICS 31-33)
- Mining, Quarrying, and Oil & Gas Extraction + Utilities (NAICS 21 and 22)
- Professional, Scientific and Technical Services (NAICS 54)
- Public Administration (NAICS 92)
- Retail (NAICS 44 and 45)

The most common data class that is compromised is Personal data and ranks number one in 7 of the 11 industries that received additional attention in the DBIR. In 4 of the 11 industries, personal data ranked second. Ironically, personal data was disclosed more frequently than healthcare data in the Healthcare industry. That makes personal data featuring in the top 2 most breached data for all 11 industries mentioned.

Credentials are present in the top 2 spots for 9 out of the 11 industries examined in depth. Only the Healthcare sector and Information sector listed credentials third. Industries where credentials were breached more often than any other data type is Accommodation and Food Services, Mining, Quarrying and Oil & Gas Extraction + Utilities, Professional Services, and Retail.

Very small businesses also received a special mentioned. Very small businesses are defined as businesses with 10 or less employees. Credentials are the most representative data type, present in 93% of all breaches in the very small business category. This business size category suffers badly under the heel of cybercrime with ransomware being the most ruthless. BEC is also featured in breaches suffered by very small businesses.

Finally, a look at geographical regions. Europe, Middle East and Africa (EMEA) contributed 1,093 incidents with 307 confirmed data breaches. The biggest motivator for threat actors is financial gain (79%) followed by espionage (21%). The top threat actor is external (97%) to the business followed by internal actors (3%) when looking at breaches. Credentials and internal data are jointly tied for first spot as the most disclosed data type. Ninety seven percent of breaches consist of System Intrusion, Social Engineering, and Basic Web Application Attack patterns.

Asia Pacific is a large geographic area and contributed 4,114 incidents with 283 confirmed data disclosures. The top actor motives include financial (54%), but espionage is a close second (46%). Unsurprisingly external threat actors are the main culprits in 98% of all breaches. Credentials (72%) is the number one stolen data variety, followed by Internal data(26%) and Secrets (18%). Ninety eight percent of all breaches include Social Engineering, Basic Web Application Attacks and System Intrusion as top patterns. Where social attacks were used, phishing is present in 99% of these incidents. Defacements are also popular in this region with 2,800 recorded.

North America is the biggest contributor to the caseload of 2021 with 4,504 incidents and 1,638 confirmed breaches. The most common data type compromised is Credentials. External attackers represent the largest threat (90%). The top patterns for 90% of breaches include System Intrusion, Social Engineering, and Basic Web Application Attacks. Financial gain was the leading actor motivator by far.

Latin America and the Caribbean (LAC) was also present but with a relatively small data set. LAC contributed 92 incidents of which 24 are confirmed data disclosures. The number one actor motive was financial gain (92%), followed by Convenience (3%), Espionage (2%), Grudge (2%), and other (2%) for all incidents. External threat actors (95%) are the main cause of incidents in LAC. The types of data compromised include System (51%), Credentials (40%), Internal (21%) and other (12%). The top patterns in 88% of all incidents include System Intrusion, Denial of Service and Social Engineering.