CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

December 15, 2022

2022 Adversary Infrastructure Report

Recorded Future's Insikt Group® conducted a study of malicious command-and-control (C2) infrastructure identified using proactive scanning and collection methods throughout 2022. All data was sourced from the Recorded Future® Platform and is current as of September 1, 2022.

Executive Summary

Recorded Future tracks the creation and modification of new malicious infrastructure for a multitude of post-exploitation toolkits, custom malware, and open-source remote access trojans (RATs). Since 2017, we have created detections for 108 families including RATs, advanced persistent threat (APT) malware, botnet families, and other commodity tools. We observed over 17,000 unique command-and-control (C2) servers during 2022, which is up 30% from last year. Much like 2021, our collection in 2022 was dominated by Cobalt Strike team servers, botnet families including IcedID and QakBot, and popular RATs such as PlugX.

Key Judgments

- 32% of detected servers (5,481 servers) were identified exclusively by Recorded Future's Command-and-Control source.
- We observed an average of a 33-day lead time between when a C2 server is detected by our scanning efforts and when it is reported in other sources.
- The overall number of detected C2 servers increased by 30% from 13,629 in 2021 to 17,233 in 2022.
- PlugX remains in heavy use despite ShadowPad being touted as its "successor".
- Much like in 2021, botnet malware, mainly Emotet and QakBot, have continued to expand their C2 infrastructure and remain prevalent throughout the year.
- Shifts in Russian state-sponsored C2 infrastructure can make tracking specific operations more difficult than with other state-attributed entities.
- The largest hosting providers continue to have the most C2 server observations, as expected. However, there have been shifts in which providers are being used for C2 servers, including a more than 300% increase in hosting on Shenzhen Tencent Computer Systems that made it the most popular for C2s in our survey, with China overtaking the US as the top country by volume for C2 server-hosting.
- In 2021, we predicted a more diverse C2 environment where we would see an increase in detections from new tooling. However, the variety we observed came more from a broader spread of established tooling rather than from the use of new tools.

Background

Increasing notification lead time in the identification of soon-to-be activated malicious command-and-control (C2) servers can help defenders more proactively neutralize threats. Before a C2 server can become operational, there are several steps a threat actor needs to take as seen in Figure 1. First, the server infrastructure has to be acquired, either via compromise or legitimate purchase. Next, if a domain name is required for C2 communications, it will have to be acquired and registered. Then, the software must be installed, configurations tuned, transport layer security (TLS) certificates registered (if applicable), and files added to the server. The actors must access it via panel login, secure shell (SSH), or remote desktop protocol (RDP), and then expose the malware controller on a port to allow the data to transfer from the victim and to administer commands to infections. (Depending on the operation, additional actions may also be required.) Only after these steps are completed can the server be used maliciously.

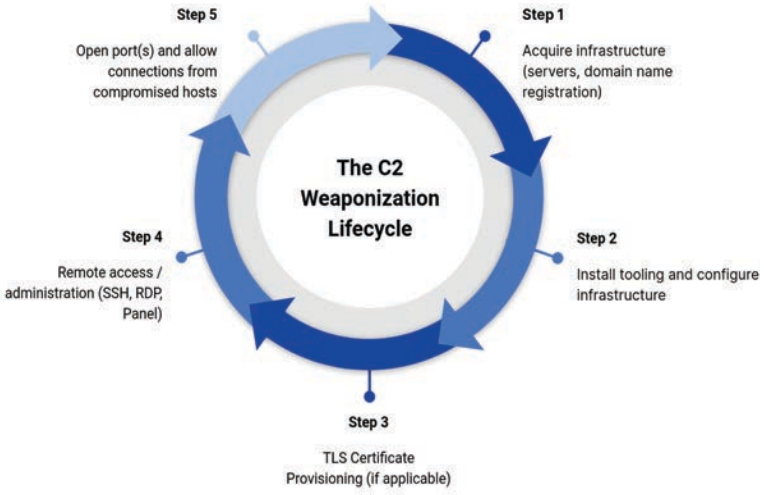

Figure 1: *C2 Weaponization Lifecycle (Source: Recorded Future)*

However, in standing up, configuring, and accessing the server, the adversary leaves behind artifacts that are observable prior to the use of the server in a phishing campaign or with a malicious tool. These artifacts create detection opportunities for defenders, and include software versions deployed on the server, the login panel, TLS certificate patterns, or the default message returned by a simple probe.

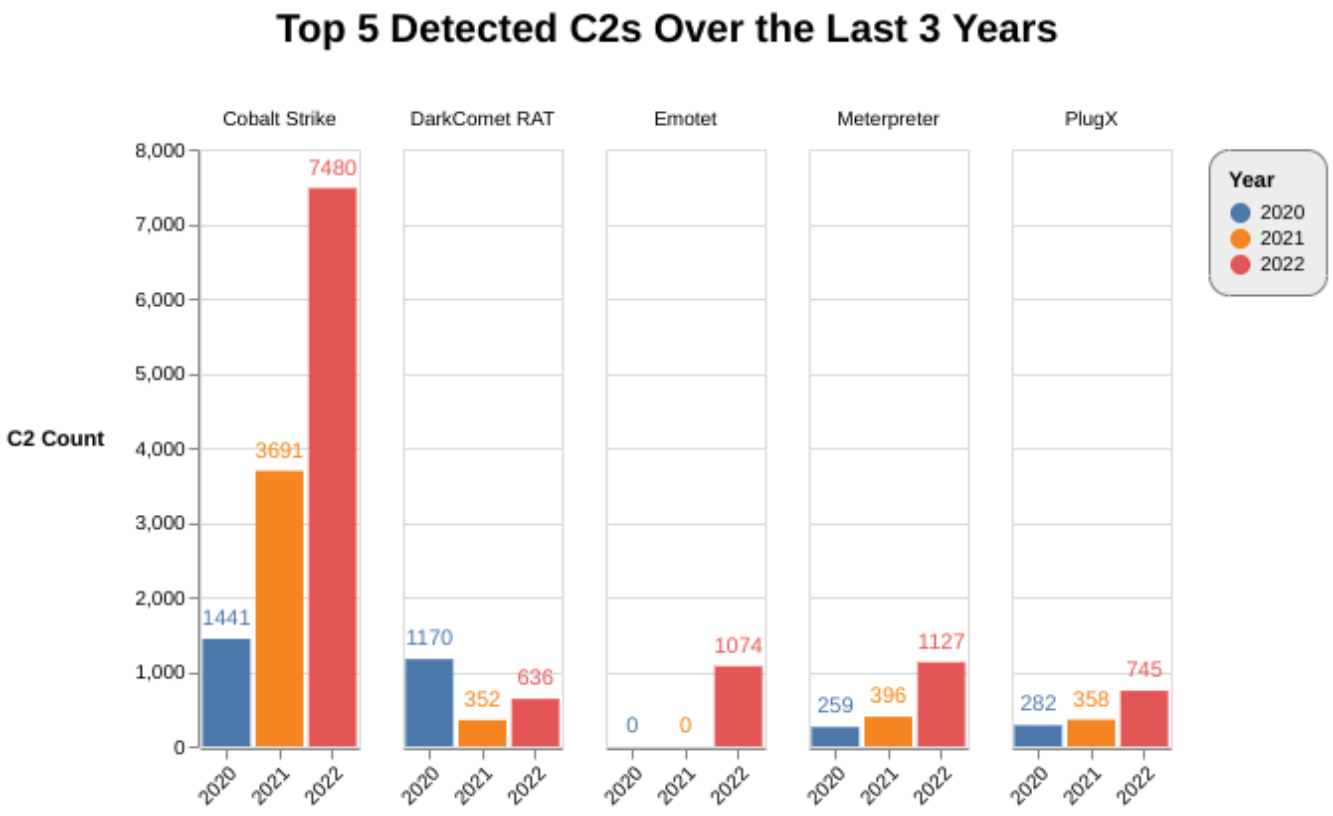

Figure 2: *3-year trends for top 5 C2s observed by Recorded Future (Source: Recorded Future)*

Detecting C2 servers from creation to weaponization provides insight into how adversaries conduct malicious campaigns. This includes:

- Comparing C2 detections to reports of intrusions related to those families can identify how many intrusions are caught and potentially how many events remain unknown in the public domain.
- Measuring the tempo of server creation can provide insight into forthcoming surges or drawdowns of activity.
- Capturing indicators and intelligence otherwise unavailable in the public domain.

A Note on Collection Bias

Recorded Future collects information about C2 servers based predominantly on traits from known malware families and their server-side software. The nature of this collection is focused on identifying known command-and-control frameworks and their derivatives or support infrastructure and includes passive and active internet scan data. We only verify that an IP address is a C2 server with proof of malicious activity from the C2. Therefore, we will be biased in reporting servers of known threats, and have a collection bias towards those servers. This methodology should not act as a replacement for identifying anomalies or detecting odd traffic inside a network.

Threat Analysis

Our top 5 C2 family observations are not dominated by any one malware category and instead have a mix of post-exploitation frameworks (Cobalt Strike), remote access tools / backdoors (PlugX, DarkComet), and botnets (Emotet).

A closer look at the top 5 families over the last 3 years shows the continuous rise in the number of Cobalt Strike, Meterpreter and PlugX servers we identified, despite the age of these tools. Our detection for Emotet has been active for about a year, and based on the number of detections we have observed, Emotet is indeed back in full operation. DarkComet remains relevant as evidenced by its increase of ~47% over the prior year. New malware and red-teaming tools are released every year; however, we observe less usage of them as compared with entrenched tools of the prior generation, as seen in Figure 2.

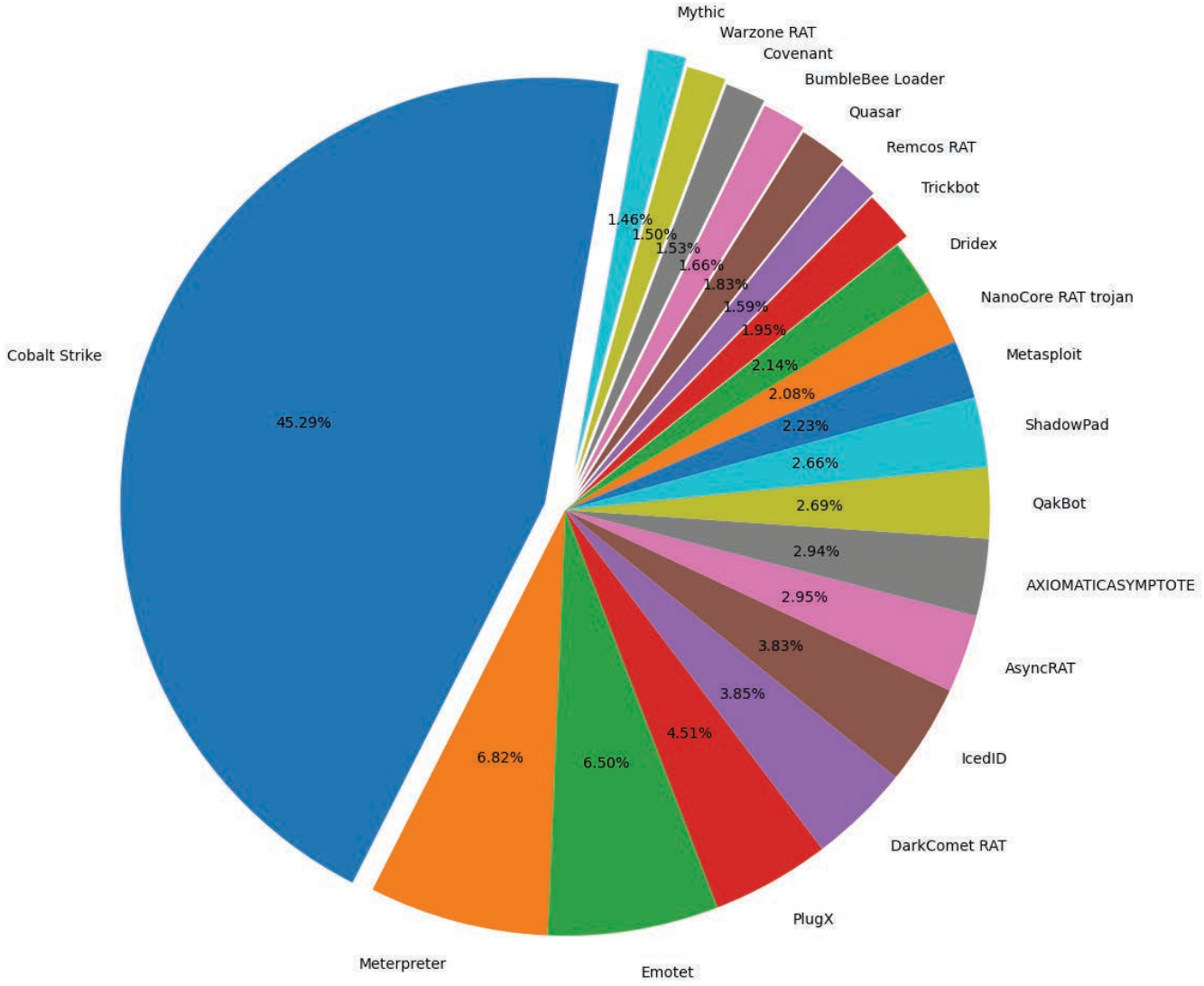

Figure 3: *Total C2 detections by malware family as seen by Recorded Future (Source: Recorded Future)*

When expanding the scope into the top 20 C2 detections we see a more well-rounded C2 environment including new families, such as Brute Ratel (BRc4) and BumbleBee alongside mainstays such as PlugX, AsyncRAT, IcedID and DarkComet. In 2021, we predicted that "the C2 environment will continue to diversify. As new malware families and C2 frameworks are released, we anticipate a portion of them will be aware of threat intelligence measures to scan and detect their servers". While it is true that in 2022 we have observed a significant increase in the number of C2s we detected for tools outside last year's top 5 and top 20, most of the increase this year is due to the use of "established" tooling such as PlugX, Remcos, DarkComet, and QuasarRAT by a wider array of actors. The top 6 tools in our data set with increased usage in 2022 as compared with 2021 were:

1. PlugX (51% increase)
2. Remcos (51% increase)
3. DarkComet (44% increase)
4. QuasarRAT (40% increase)
5. Mythic (33% increase)
6. AsyncRAT (24% increase)

We believe this high level of commodity tool use indicates that an increasing percentage of threat actors are more concerned with blending in and being non-attributable rather than being undetectable, or have simply determined that their targets are not likely to detect even these well-known tools. Additionally, considering the cost and expertise required to develop bespoke tooling, threat actors may prefer buying commodity tools or using free open-source tools.

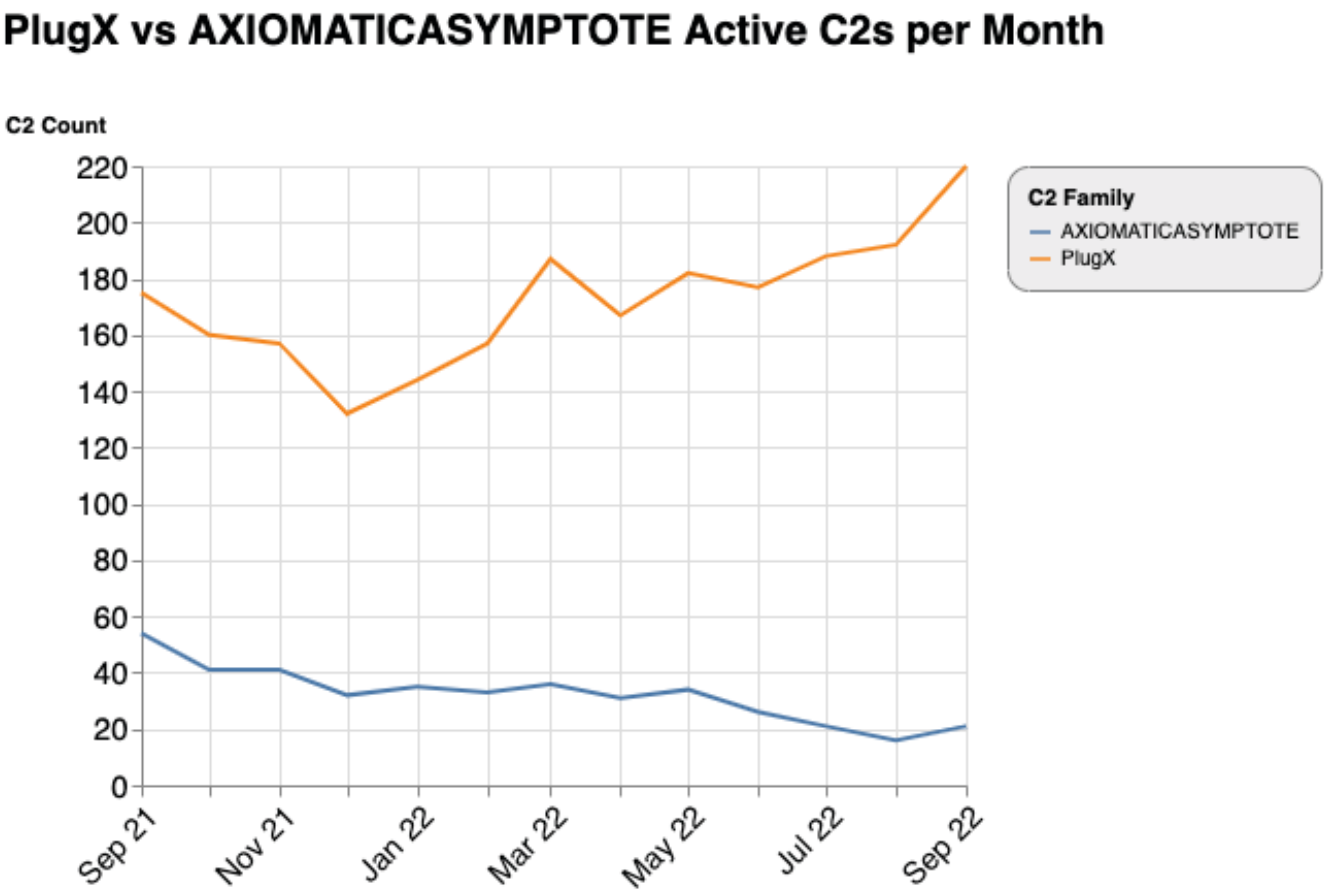

Figure 4: *Count of PlugX and AXIOMATICASYMPTOTE C2s detected over the past 12 months (Source: Recorded Future)*

For example, use of BRc4 will provide more endpoint detection and response (EDR) evasion techniques, but poses more risk to attribution due to its smaller user base, whereas use of DarkComet may not be as stealthy or evasive but is an open-sourced RAT that is used by many threat actors.

2022 Adversary Infrastructure Themes

When looking at our C2 observations as a whole, we identified 3 top themes for 2022:

1. PlugX Remains Successful, in Spite of Its Successor: PlugX is still widely used, despite ShadowPad being touted as its "successor".
2. Back to Bots (Again and Again): While not quite as prevalent as in 2021, multiple botnets are still very active; Emotet, IcedID, QakBot, Dridex, and TrickBot all made the top 20 in 2022.
3. Russia, Burn after Reading: The limitations of Russia-attributed C2 detections.

PlugX Remains Successful, in Spite of Its Successor

In our 2020 Adversary Infrastructure report, we referenced an article from Doctor Web that described ShadowPad as the successor to PlugX. We continued to observe PlugX infections after 2020, despite the increased adoption of ShadowPad by multiple Chinese state-sponsored groups (Recorded Future tracks the infrastructure that administers ShadowPad controllers as AXIOMATICASYMPTOTE). In 2022, usage of PlugX continues and has even increased as shown in the graph below.

PlugX has been used by primarily China-based threat actors over the past decade. A builder for an earlier PlugX variant was leaked publicly as reported by Airbus in 2015. This indicates that PlugX usage is likely less-closely controlled compared to ShadowPad, which is likely privately sold to a limited set of Chinese state-sponsored threat actors. We actively track PlugX variants attributed to the RedDelta and RedFoxtrot threat actor groups.

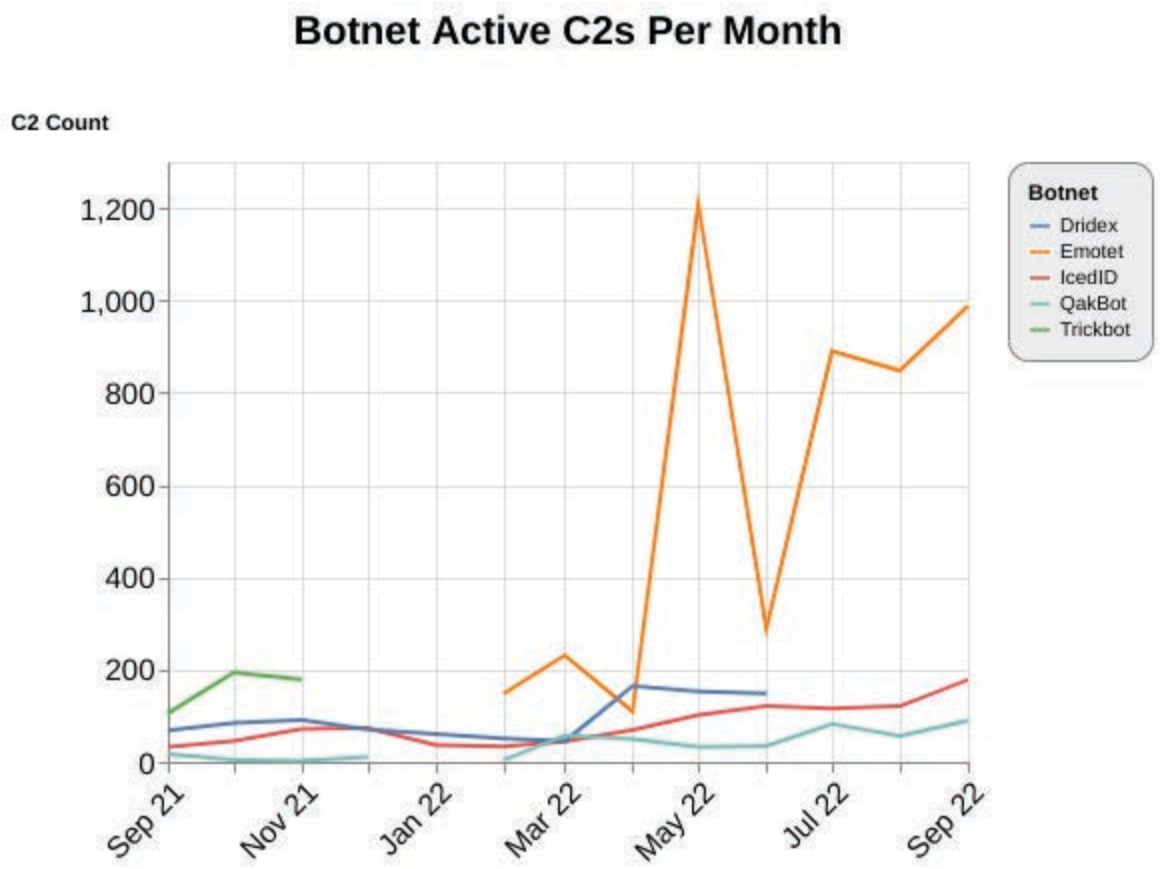

Figure 5: *Comparison of detected Dridex, Emotet, IcedID, QakBot, and TrickBot C2s (Source: Recorded Future)*

Back to Bots (Again and Again)

In 2021 we saw a sharp increase in botnet activity after the Emotet takedown, with TrickBot, QakBot, Bazar, IcedID, and Dridex representing the majority of the C2s we detected. In 2022, while botnets did not dominate our C2 data, they were still present in our top 5 and top 20 lists. As shown in Figure 5, Dridex, Emotet, IcedID, QakBot, and TrickBot are the botnet families we observed with the most C2 detections this year.

TrickBot and Dridex

We observed a spike in the number of TrickBot C2s detected in October 2021 (194 active C2s) before the malware went dormant a few months later; similarly, Dridex activity remained steady, ranging from 45 to 80 active C2s per month until a spike in June 2022 (150 active C2s), prior to going dormant.

The TrickBot activity aligns with reporting at the start of this year noting that TrickBot operators are phasing out the use of the TrickBot malware. For Dridex, the increased use in March up to the spike in June correlates with reporting of Dridex being used in RIG exploit kits. The sudden dormancy of Dridex could also be indicative of the botnet being surpassed overall due to the prevalence of IcedID and QakBot, and the resurrection of Emotet.

QakBot

The number of QakBot C2s observed was relatively low at the end of last year and into this year, with an average 10 active C2s per month. Starting in March 2022, we have observed a significant increase in the number of QakBot C2s detected, with the highest being 90 active C2s in September 2022. Most recently, SentinelOne has seen QakBot being used to deliver Black Basta ransomware.

IcedID

Up until May 2022, we have observed IcedID having anywhere from 30 to 60 active C2s per month. Starting in May we see an increase up to 102 and a further steady increase to 178 active C2s in September 2022. The following key events may be contributing factors to these increases:

- In April 2022, CERT-UA sent an advisory about a mass distribution of XLS documents that install the IcedID malware.
- Most recently, IcedID has reportedly been used to download and execute Quantum Locker ransomware.

Emotet

After the takedown of Emotet infrastructure in early 2021 and a long break in activity, there was speculation that Emotet may cease operations permanently; this proved to be incorrect. Emotet returned in late 2021, reportedly in coordination with the Conti ransomware operation. Emotet's early resurgence was reported to be a reuse of TrickBot's infrastructure. Coincidentally, in Figure 5, we can see Emotet starts off with the same number of active C2s we tracked for TrickBot right before the latter ceased operations.

Although the volume of Emotet C2s was relatively low in late 2021 and early 2022, we observed a major spike in May 2022 with over 1,200 active C2s. Reporting from Netskope Threat Labs mentions 2 active campaigns in this timeframe that were using LNK files and Microsoft Office documents to spread Emotet.

In June the numbers returned to a low range until July 2022, at which time Emotet numbers began rising again. The number of active Emotet C2s observed at present are almost to the level of the surge seen in May, with just over 1,000 active C2s in September 2022. The recent uptick in Emotet active C2s since July 2022 supports the most recent reporting on Emotet:

- Emotet is being used to load Quantum and ALPHV ransomware.
- Proofpoint stated that Emotet is distributing "hundreds of thousands" of phishing emails a day in November, and is being used to load and execute IcedID. Increased distribution of IcedID via Emotet may also contribute to the recent uptick in our IcedID detections.

Russia, Burn after Reading

Based on our observations, Russian state-attributed actors often use better operational security for C2 infrastructure when compared with other state-sponsored operations. For instance, they often use methods such as operating C2 servers on a 1-to-1 basis, thus only interacting with implants at a single target organization. We also observe that when their C2 infrastructure is publicly reported upon, it is often quickly dispensed with. Some Russian state-sponsored actors have also been at the forefront of the overall trend of state actors shifting toward usage of commodity malware and popular C2 frameworks. Threat actors taking advantage of common, off-the-shelf software for espionage operations can make attribution more difficult for researchers and investigators.

In contrast, operations attributed to China, Iran, and some other states are often incautious with their malware and infrastructure operational security, using specific C2s for numerous targets and after public disclosure, or using what is essentially the same malware (such as PlugX) for years while sharing it among multiple operational teams.

Frequent shifts in Russian state-sponsored C2 infrastructure can make tracking specific operations more difficult. GRAVITYWELL, the Recorded Future designation for server technology and TLS certificate configuration commonly used to host the Russian Foreign Intelligence Service (SVR)-linked WellMess backdoor, provides an example of such transient infrastructure.

We have tracked GRAVITYWELL through multiple phases. Between these phases, we have observed distinct shifts in infrastructure soon after public disclosures of GRAVITYWELL activity.

In July 2020, the UK's National Cyber Security Centre (NCSC) published a report on APT29 operations using WellMess. The report included the C2 infrastructure known to be in use in the campaign. In August 2020, that infrastructure was replaced with a new set of C2s, identifiable by TLS certificate patterns that were distinct from the previous phase of the campaign. In July 2021, a RiskIQ report was released that identified more than 30 C2 servers that provided TLS certificate details. As happened a year earlier, changes in those C2s were observed within a month of the report's release.

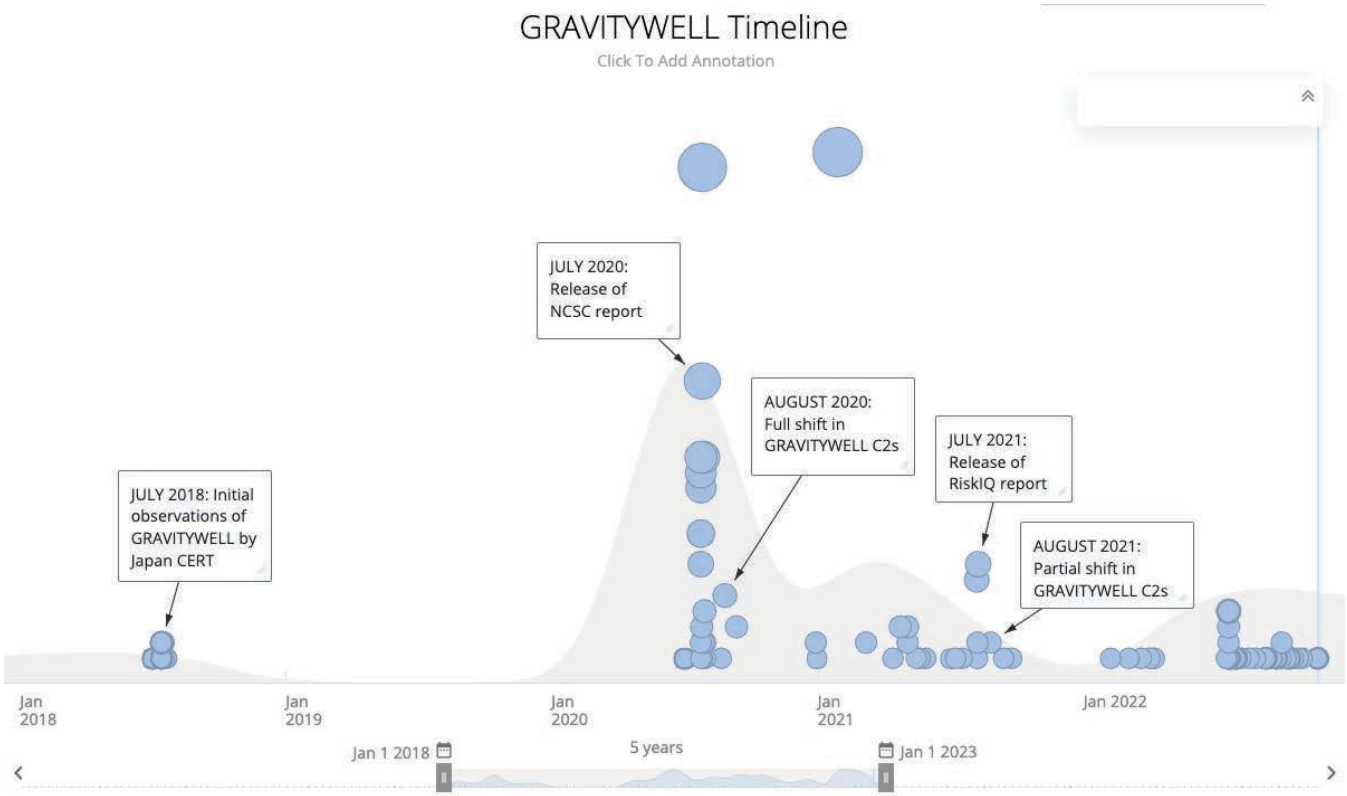

Figure 6: *Timeline of GRAVITYWELL public reporting and Infrastructure changes (Source: Recorded Future)*

Post-exploitation Frameworks

It is difficult to estimate what percentage of any of the post-exploitation frameworks we detected are used in legitimate red-teaming operations, and which are used by criminal or espionage elements. Overall, volume changes may also be tied to improved signatures and increased collection efforts in addition to adoption in various operations.

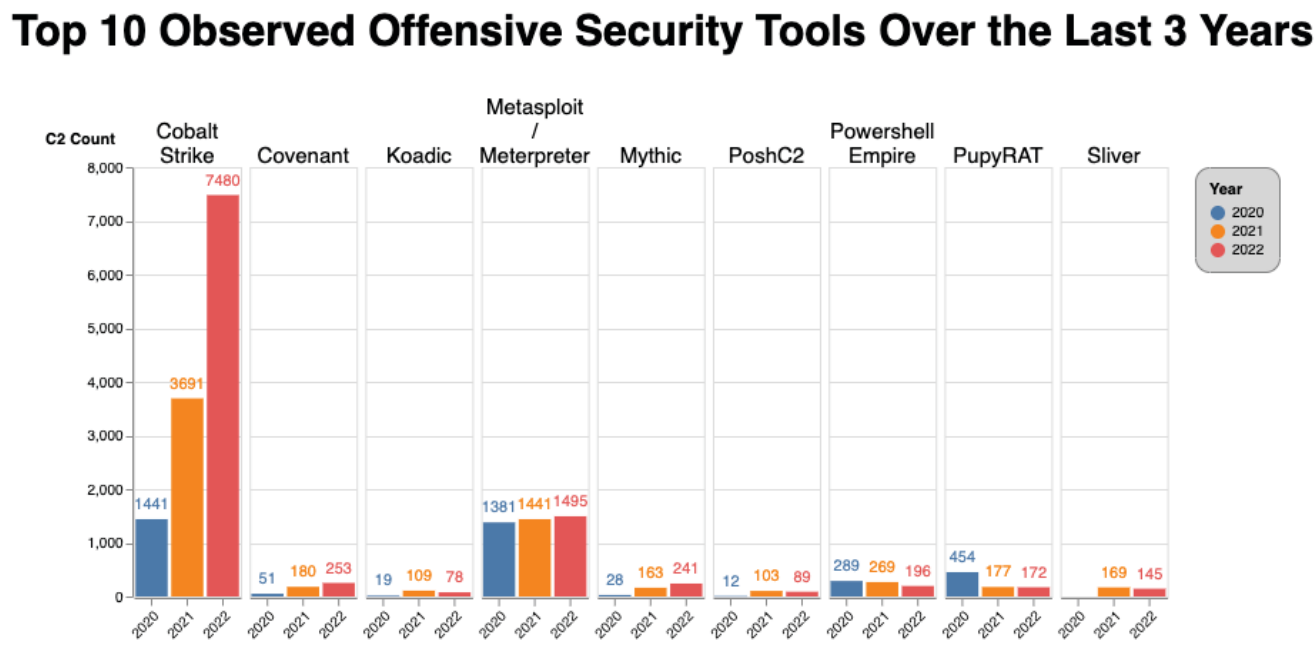

Figure 7: *C2 observations for offensive security tools over the past 3 years (Source: Recorded Future)*

Comparing the top 10 offensive security tools that we observed this past year against the prior 2 years shows one thing very clearly: Cobalt Strike C2 activity continues to increase at a rapid pace. Cobalt Strike is clearly the preferred offensive security tool for an array of actors, and Cobalt Strike detection volume increased significantly last year. We attribute the 2-fold increase to the multitude of detections, the length of time those detections have been running, and the volume of actors using Cobalt Strike.

Other frameworks in our top 10 with increased volume include Covenant, Mythic, and Metasploit/Meterpreter (these 2 were combined this year); however, none of them jumped as significantly as Cobalt Strike. Covenant's open-source project has not been updated since 2021, but continues to see an uptick in usage. Mythic continues to receive updates to its code base. Some Mythic infrastructure references the name Botleggers Club, which is also mentioned in the Conti Leaks, suggesting that at least some ransomware operators were using it.

Both Brute Ratel (BRc4) and BeEF are honorable mentions this year as their detection rates were not yet high enough to make it into the top 10. The developer behind BRc4, who has a background in EDR development, strives to make the tool harder to detect by specifically targeting the way EDRs work to avoid detection. A version of BRc4 has been cracked and is spreading through the criminal underground as well, and has been seen in use by the Black Basta ransomware gang.

Global Scale

We detected 30% more C2 servers in 2022 (17,233) as compared with 2021 (13,268) as a result of: the development of detections for new malware families; improvements in detections for existing malware families; and increased use of tools we have detections for such as Cobalt Strike, Meterpreter, and PlugX.

We observed the creation of C2 infrastructure on 1,419 hosting providers across 116 different countries. While this represents a majority of global geography, the abused servers account for only a small percentage of the total autonomous systems (AS) operators, which exceeds 70,000 providers.

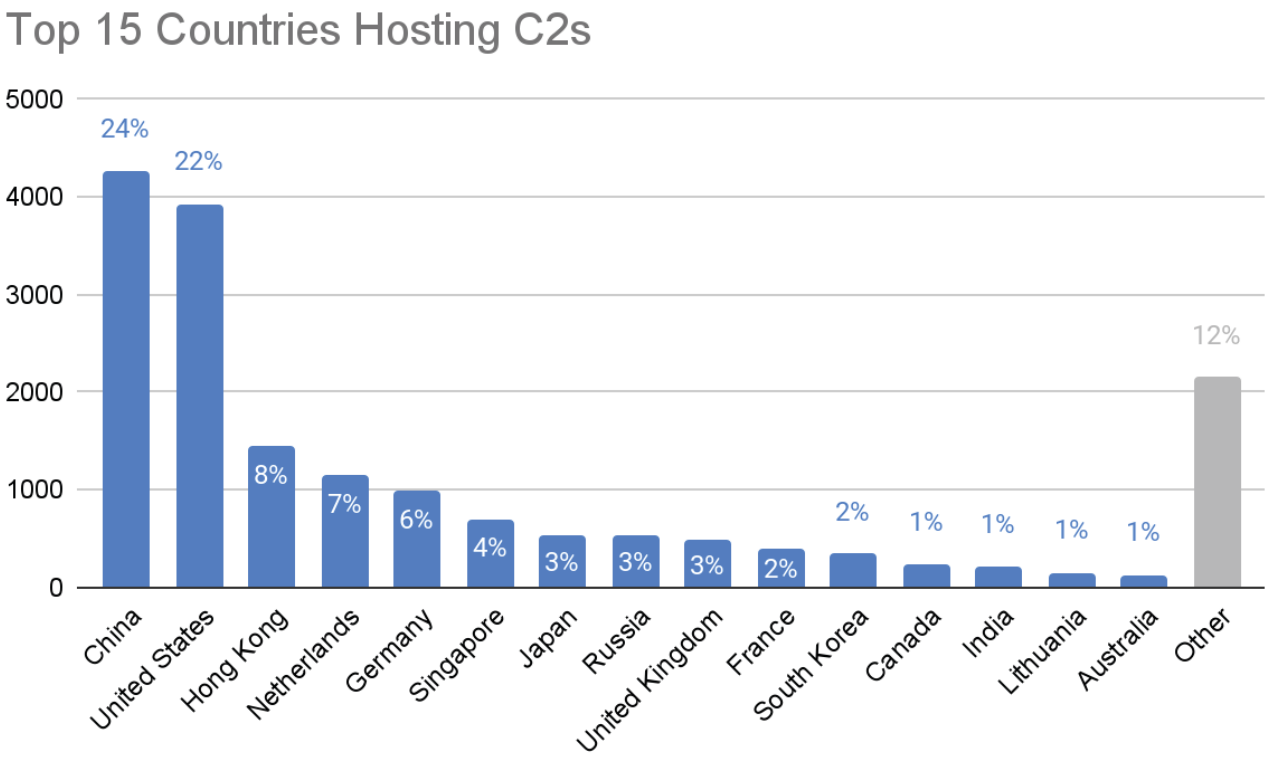

Figure 8: *C2 observations by country (as identified by autonomous systems number [ASN] location) (Source: Recorded Future)*

- As in 2021, the largest hosting providers are the most abused for C2 hosting; 24 AS operators (1% of total autonomous systems numbers [ASN] observed) had more than 100 C2 servers detected on them during 2022 (as opposed to 20 AS operators in 2021).
- While we observed 1,419 unique AS operators hosting C2 servers during 2022, the great majority were observed hosting 100 or fewer C2 servers (98%); 1,225 AS providers (86% of total ASNs observed) hosted 10 or fewer C2 servers, and 682 AS operators hosted only 1 C2 server.
- China hosted 4,265 C2 servers in 2022, the US was second with 3,928, and Hong Kong was third with 1,451, with these top 3 countries accounting for 55% of all detected C2 servers; the top 10 countries account for 88% of all detected C2 servers.
- 18 of the 116 countries observed hosting C2 servers hosted only 1 C2 server during 2022.
- While the US share of C2 servers dropped from 34% to 22%, China's shares increased from 14% to 24% mostly due to substantial increase in C2 detections at Chinese hosting provider Shenzhen Tencent Computer Systems.
- The share of C2 servers detected in Hong Kong and the Netherlands went up from 3.3% to 8% and 2.1% to 7%, respectively.

While there were slight changes in the ranking order, the composition of the top 10 C2 hosting providers by volume remained mostly unchanged since 2021; only Singapore-based BGPNET Global (AS64050) dropped out due to a decrease from 181 to 147 C2s and was replaced by Alibaba (US) Technology Co., Ltd. Overall, all top 10 C2 hosting providers recorded substantial increases in the number of detected C2 servers, with 4 of them recording increases of more than 50% between 2021 and 2022.

Top 10 C2 Hosting Providers by Volume					
Hosting Provider	**ASN**	**Country**	**Total C2s (2021)**	**Total C2s (2022)**	**YoY Increase**
Shenzhen Tencent Computer Systems	AS45090	China	571	2297	+302%
DigitalOcean, LLC	AS14061	United States	968	1421	+48%
Amazon.com, Inc.	AS16509	United States	624	1156	+85%
Hangzhou Alibaba Advertising Co., Ltd.	AS37963	China	574	1126	+96%
The Constant Company, LLC	AS20473	United States	700	834	+19%
Microsoft Corporation	AS8075	United States	205	411	+100%
OVH SAS	AS16276	France	267	338	+27%
Linode, LLC	AS63949	United States	208	291	+40%
M247 Ltd	AS9009	United States	171	228	+33%
Alibaba (US) Technology Co., Ltd.	AS45102	United States	95	192	+102%

Table 1: *Top C2 hosting providers by volume of C2 servers observed during 2022 and compared to 2021*

- Shenzhen Tencent Computer Systems, operating out of China, recorded an increase of 302% in C2 servers and ended up hosting the most C2 servers of any of the ASNs observed by Recorded Future in 2022. The hosting provider accounted for 2,297 individual C2 servers (13%). The most commonly observed family on Shenzhen Tencent Computer Systems was Cobalt Strike, with 2,032 servers identified.
- The next largest was DigitalOcean LLC, operating out of the United States, which had topped the list in 2021. The hosting provider recorded an increase of 48% and hosted 1,421 individual C2 servers (8%). The most commonly observed family on DigitalOcean LLC was Cobalt Strike, with 526 servers identified.

Table 2 shows that the top 5 malware families accounted for a major percentage of C2 servers on the top 10 hosting providers; our top 5 malware families accounted for at least 80% of all C2 servers detected on half of the top 10 hosting providers. The “Top Malware %” column reflects the percentage of C2 detections that the top 5 malware families contributed to the total C2s for the hosting provider.

Top 5 Malware Families by C2 Hosting Providers			
Hosting Provider	**Top Families**	**Total C2s**	**Top Malware %**
Shenzhen Tencent Computer Systems	Cobalt Strike, Meterpreter, AXIOMATICASYMPTOTE, Metasploit, PlugX	2178	95%
Hangzhou Alibaba Advertising Co., Ltd.	Cobalt Strike, Meterpreter, Sliver, PupyRAT, XtremeRAT	1041	92%
DigitalOcean, LLC	Cobalt Strike, YerLoader, IcedID, Meterpreter, Mythic	935	66%
Amazon.com, Inc.	Cobalt Strike, Meterpreter, Koadic, Sliver, Gh0st RAT	668	58%

Top 5 Malware Families by C2 Hosting Providers			
Hosting Provider	**Top Families**	**Total C2s**	**Top Malware %**
The Constant Company, LLC	Cobalt Strike, PlugX, AXIOMATICASYMPTOTE, Meterpreter, QakBot	669	80%
Microsoft Corporation	Cobalt Strike, Cerberus, Meterpreter, DarkComet, Empire Powershell	290	71%
M247 Ltd	Cobalt Strike, BumbleBee, IcedID, Meterpreter, PlugX	200	88%
OVH SAS	Cobalt Strike, BumbleBee, IcedID, Meterpreter, NanoCore RAT	178	53%
Alibaba (US) Technology Co., Ltd.	Cobalt Strike, Meterpreter, XtremeRAT, AXIOMATICASYMPTOTE, CROSSWALK	159	83%
Linode, LLC	Cobalt Strike, Meterpreter, AXIOMATICASYMPTOTE, Mythic, PlugX	125	43%

Table 2: *Top malware families by C2 hosting providers observed during 2022*

Cobalt Strike is the top malware family on all hosting providers in Table 2, followed by Meterpreter in many cases. AXIOMATICASYMPTOTE and PlugX are typically found on the same hosting providers. 26% of Recorded Future's BumbleBee detections were on M247 Ltd and OVH SAS, while 57% of Cerberus detections were found on Microsoft Corporation infrastructure.

While these hosting providers accounted for the largest number of C2 servers, the C2 servers represented a minuscule percentage of total number of servers under their jurisdiction. Table 3 highlights the 10 providers with the highest percentage of C2 servers compared to their total holdings. This estimate is based on the number of IPv4 prefixes announced by the AS, compared to confirmed C2 servers observed in 2022.

- The only 2 hosting providers from Table 3 that had already been part of the list of top 10 hosting providers with the highest percentage of C2 servers hosted in 2021 were International Hosting Solutions LLP, operating out of the United Kingdom, and HDTIDC LIMITED, operating out of Hong Kong. Various bulletproof hosting providers such as Media Land LLC or Host Sailor Ltd. dropped out of the list.
- Based on open-source data, most hosting providers from Table 3 are either:
  - associated with risky web traffic (as with UAB Cherry Servers, BL Networks, or KURUN CLOUD INC, for example);
  - have previously been regarded as a preferred hosting provider by specific threat actors (for example, TAG-26 using HDTIDC LIMITED); or
  - are known bulletproof hosting providers (for example, Flyservers S.A. or Chang Way Technologies Co. Limited).

Hosting Providers with Highest Percentage of C2s Hosted				
Hosting Provider	**ASN**	**Country**	**Top Detection**	**% of Servers Hosted Are C2s**
UAB Cherry Servers	AS59642	Lithuania	Cobalt Strike	3.91%
SteamVPS SRL	AS50578	Romania	IcedID	2.73%
KURUN CLOUD INC	AS395886	United States	Cobalt Strike	2.34%
Flyservers S.A.	AS48721	Panama	Cobalt Strike	1.56%
HDTIDC LIMITED	AS136038	Hong Kong	Roaming Mantis	1.20%
International Hosting Solutions LLP	AS213354	United Kingdom	YerLoader	1.17%
Flyservers S.A.	AS209588	Panama	Cobalt Strike	0.95%
Chang Way Technologies Co. Limited	AS57523	Hong Kong	Cobalt Strike	0.91%
BL Networks	AS399629	United States	Cobalt Strike	0.80%
BlueVPS OU	AS62005	Estonia	IcedID	0.78%

Table 3: *Hosting providers who hosted the highest percentage of C2 servers compared to total servers during 2022*

Outlook

In 2023 one would likely predict that Cobalt Strike and botnets will still occupy the majority of our C2 observations. While we expect Cobalt Strike to remain in our top 5 detections for next year, we do not predict to see another 2-fold increase. We believe that Cobalt Strike usage will be cannibalized by BRc4 usage. As a result, we predict that BRc4 usage and C2 detections will increase, due to threat actors moving to use BRc4 because it aims to be less detectable by EDR agents and serves as a capable alternative to Cobalt Strike. It is also conceivable that there will be an increase in C2 observations associated with niche C2 tools such as Sliver, DeimosC2, Alchimist, and Manjusaka.

We are already seeing malware families such as Redline Stealer, QakBot, and Nanocore be successful despite their use of random and non-standard ports. This prohibits traditional, full internet scanning as it is not feasible to scan all possible non-standard ports across the IPv4 space. While once thought to be easier to detect, the use of high ports seems to still be an adequate C2 communication channel, and we predict that more C2 operators will make use of high ports for their C2 communication.

In June of 2022, ShadowServer detailed their methodology for scanning the IPv6 internet space. We predict that more organizations, including Recorded Future, will increase IPv6 scanning with resulting findings of more IPv6 C2 detections. While not widely reported on, malware that communicates over a IPv6 connection does exist, such as VirtualPie as reported on by Mandiant.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.