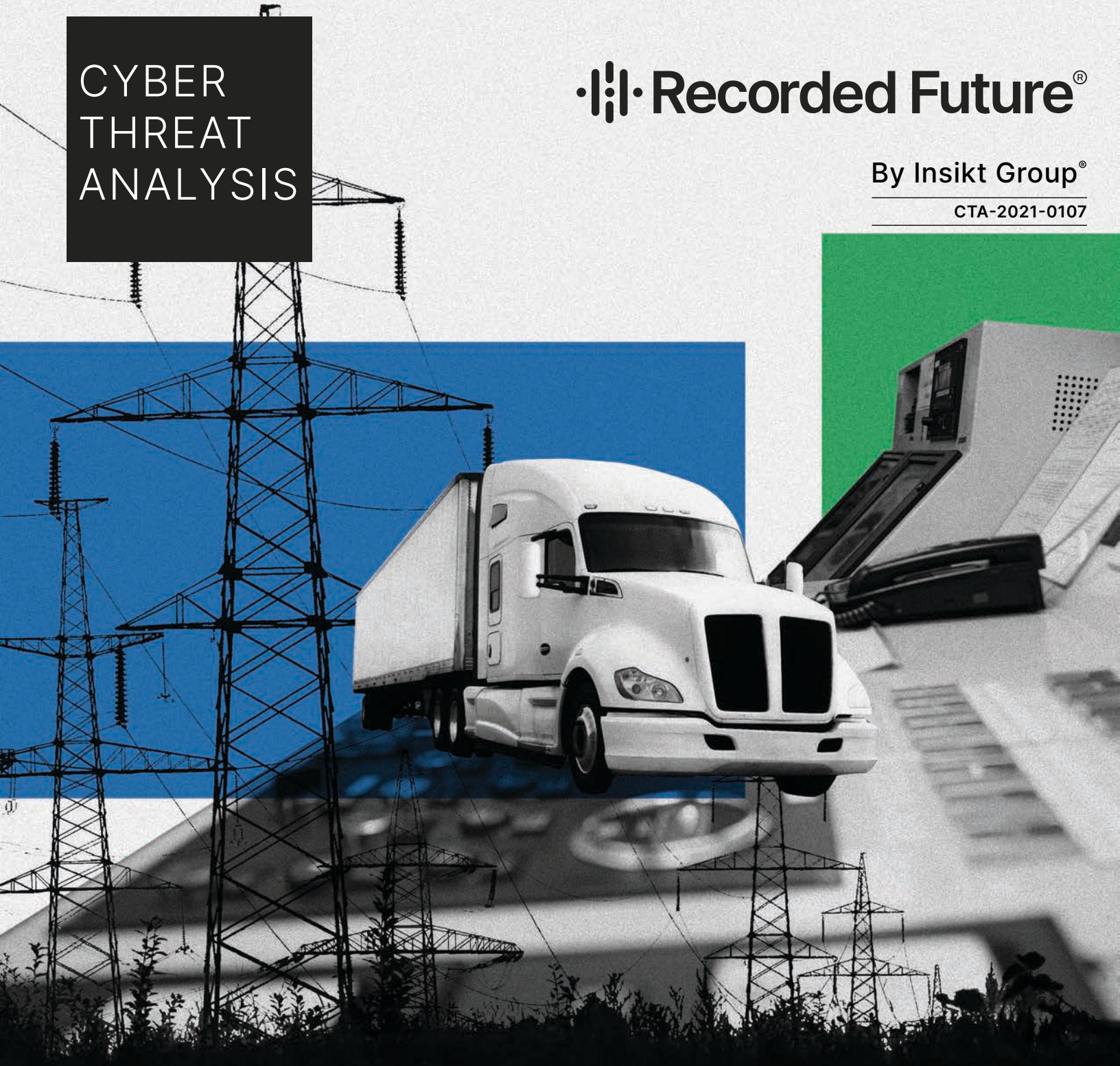
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0107



ADVERSARY INFRASTRUCTURE REPORT 2020: A DEFENDER'S VIEW

Recorded Future®

Recorded Future's Insikt Group® conducted a study of malicious command and control (C2) infrastructure identified using proactive scanning methods throughout 2020. All data was sourced from the Recorded Future® Platform. Data in this report is as of November 15, 2020.

Executive Summary

Recorded Future tracks the creation and modification of new malicious infrastructure for a multitude of post-exploitation toolkits, custom malware frameworks, and open-source remote access trojans. The effort has been ongoing since 2017, when Insikt Group created methodologies to identify the deployments of open-source remote access trojans (RATs). Recorded Future collected over 10,000 unique command and control servers during 2020, across more than 80 families.

Key Findings

- Over 55 percent of detected servers (5,740 servers) were not referenced at all in open sources; they were only identified in a proprietary Recorded Future list of command and control servers.
- On average, command and control servers had a lifespan (that is, the amount of time the server hosted the malicious infrastructure) of 54.8 days.
- Where possible, lead time was calculated if the detection was the first event for an IP address in 2020. Lead time is the length of time (in days) between when a C2 server is created, and when it is reported or detected in other sources. This identified 924 servers where lead time was generated, by comparing first sighting on the Recorded Future command and control list and its subsequent sighting on another source. Our detections had an average 61-day lead time before an IP address was found on open sources.
- Monitoring only "suspicious" hosting providers can leave blindspots, as 33 percent of C2s observed by Recorded Future were hosted in the United States, many on reputable providers.
- The hosting providers that had the most command and control servers on their infrastructure were all U.S.-based: Amazon, Digital Ocean, and Choopa.
- Detecting offensive security tools is just as important as detecting custom implants: elite operators from APT groups, human-operated ransomware actors, and common criminals use these tools to cut costs just as much as red teams do. Over 40 percent of the detections were open source tools.

Background

Lead time in identifying malicious servers can be a proactive measure in neutralizing threats. Before a server can be used by a threat actor, it has to be acquired, either via compromise or legitimate purchase. Then, the software must be installed, configurations must be tuned, and files added to the server. The actors must access it via panel login, SSH, or RDP protocols, and then expose the malware controller on a port to allow the data to transfer from the victim and to administer commands to infections. Only then can the server be used for malicious purposes.

However, in exposing, configuring, and accessing the server, the adversary leaves behind their fingerprints; sometimes in software deployed on the server, sometimes via the login panel, sometimes via SSL registration patterns. This creates an opportunity for detection, which can occur prior to a phishing email being sent or an implant getting compiled.

Similarly, such a collection can illuminate many things about adversaries. Seeing how many command and control (C2) servers are created can help one quantify the breadth of an actor's campaigns. Comparing such data to reports of intrusions related to those families can identify how many intrusions get caught, and potentially how many events remain unknown in the public domain. Finally, it can provide novel indicators and intelligence that is otherwise not available in the public domain.

Threat Analysis

The most commonly observed families were dominated by open-source or commercially available tooling. Detections of unaltered Cobalt Strike deployments (the pre-configured TLS certificate, Team Server administration port, or telltale HTTP headers) represented 13.5 percent of the total C2 servers identified. Metasploit, and PupyRAT represented the other top open-source command and control servers identified by Recorded Future.

Top 5 Most Prolific C2 Families	
Family	**2020 C2s**
Cobalt Strike	1441
Metasploit	1122
PupyRAT	454

Table 1: Top detected malware families by command and control infrastructure (These numbers include preexisting servers that were still up at the time of analysis and do not represent newly created servers in 2020).

The top 10 most common offensive security tools (OST), based on the number of observed C2 servers, included new and old families. Notably, Recorded Future observed 393 Cobalt Strike servers that were outside of common detection mechanisms; we assess these detections only represent a portion of total Cobalt Strike use. PWC and Blackberry found that a majority of Cobalt Strike deployments for which a payload was observed used cracked or trial versions of the commercially available tool.

Top 10 Observed Offensive Security Tools	
Family	**Notable Users**
Cobalt Strike	APT41, Mustang Panda, Ocean Lotus, FIN7
Metasploit	JointWorm (EVILNUM), Turla
PupyRAT	APT33, COBALT ILLUSION
Powershell Empire	Sandworm, GADOLINIUM
Meterpreter	MuddyWater, TA505
Covenant	APT34 (GreenBug)
Armitage	WIZARD SPIDER (UNC1878)[1]
Octopus C2	Unnamed Chinese APT
Sliver	N/A
Responder	APT28, APT40 (TEMP.Periscope)
PoshC2	UNC1945

Table 2: Example open source malware families tracked by Recorded Future (These numbers include preexisting servers that were still up at the time of analysis and do not represent newly created servers in 2020).

Nearly all of the OSTs detected by Recorded Future have been linked to APT or high-end financial actors. The ease of access and use of these tools, mixed with the murkiness of potential attribution makes them appealing for unauthorized intrusions and red teams alike. This, in addition to the adoption of these frameworks by ransomware actors, makes their detection a priority.

Host(er)s With the Most (C2s)

Recorded Future C2 data allowed us to identify the most popular hosting providers for C2 servers. We observed the creation of C2 infrastructure on 576 hosting providers, representing only a small percentage of the total AS operators, which exceeds 60,000 providers.

The most-used ASNs are undoubtedly linked to the size of the provider, not necessarily implying that they are bulletproof hosting providers or complicit in adversary actions. The most used tooling can be considered dual use, increasing the volume of these servers on more reputable AS ranges.

Amazon.com, Inc., operating out of the United States, hosted the most C2s of an ASN observed by Recorded Future. They accounted for 471 individual command and control servers (roughly 3.8 percent). The most commonly observed family on Amazon.com, Inc. was Cobalt Strike, with 167 servers identified. The next largest was Digital Ocean, also operating out of the U.S.

Servers in the United States that accounted for other top hosting providers can be seen below. The deployment of Cobalt Strike and Metasploit controllers on these providers is not indicative of malpractice or negligent hosting, but is more likely due to authorized red teams using these tools on cloud infrastructure.

[1] On October 29, 2020, Recorded Future detected an Armitage certificate on the IP 179.43.128[.]5, which was also hosting a Cobalt Strike server used by UNC1878, with likely intent to deploy Ryuk Ransomware.

Top 10 C2 Hosting Providers				
Hosting Provider	**ASN**	**Country**	**Top Family**	**Total C2s**
Amazon.com, Inc.	AS16509	United States	Cobalt Strike	471
Digital Ocean	AS14061	United States	Metasploit	421
Choopa, LLC	AS20473	United States	Cobalt Strike	368
Zenlayer Inc	AS21859	United States	Roaming Mantis	358
Hangzhou Alibaba Advertising	AS37963	China	Cobalt Strike	335
ICIDC Network	AS136800	China	Cobalt Strike	277
OVH SAS	AS16276	France	PupyRAT	273
Shenzhen Tencent Computer Systems	AS45090	China	Cobalt Strike	262
Google LLC	AS15169	United States	Bozok RAT	241
Space-IX - RECONN LLC	AS6870	Russia	DarkComet	205

Table 4: Hosting providers who hosted the most command and control servers during 2020.

There is less predictability in the most common ASNs used across OSTs, as they are readily available for red team exercises and unauthorized intrusions.

Top OST Hosting Providers				
Family	**Hosting Provider**	**ASN**	**Country**	**C2s**
Cobalt Strike	ICIDC NETWORK	AS136800	China	259
Metasploit	Shenzhen Tencent Limited	AS45090	China	124
PupyRAT	Digital Ocean	AS14061	United States	85
Powershell Empire	Digital Ocean	AS14061	United States	43
Covenant	Amazon.com, Inc.	AS16509	United States	29

Table 5: Top hosting providers for each OST.

Publicly available tooling published as remote access trojans (RATs) also had limited predictability of its favored hosting providers.

RATs' Favorite Hosting Providers				
Family	**Hosting Provider**	**ASN**	**Country**	**C2s**
QuasarRAT	Internap Corporation	AS19024	United States	175
DarkComet	RECONN LLC	AS6870	Russia	89
Bozok RAT	Google LLC	AS15169	United States	62
njRAT	Crnogorski Telekom	AS8585	Montenegro	32
REMCOS	Taiwan Academic Network	AS1659	Taiwan	14

Table 6: Top hosting providers for each RAT.

Recommendations

- Proactive detection creates an advantage for defenders, giving them preparatory time to ensure additional file- and network-based detections are in place.
- Recorded Future clients can rapidly identify infections by detecting IP addresses found in the Recorded Future Command and Control List.
- Recorded Future users can query any malware entity, using the source Recorded Future Command and Control List, to conduct similar research of their own.
- Employ detection-in-depth for common open source tooling via correlation searches for SIEMs for suspicious behaviors, YARA for suspicious file contents, and SNORT for suspicious or malicious network traffic.
- The detections for each family show the increased use of open source tools beyond just the families that get major publicity. These other families should be prioritized for network and host-based detection in enterprise environments.
- The adoption of lesser-known open source tooling such as OctopusC2, Mythic, and Covenant by APT and criminal adversaries highlights the need for threat intelligence practitioners to track and evaluate use of these tools.

Outlook

Over the next year, Recorded Future expects further adoption of open source tools that have recently gained popularity, specifically Covenant, Octopus C2, Sliver, and Mythic. Three of these tools had graphical user interfaces, making them easier to use for less experienced operators, and all four have verbose documentation on their uses. These tools had rapid adoption after their releases and were used by both red teams and unauthorized actors. Despite expected gains by these open source frameworks, Cobalt Strike will very likely maintain its lead atop our detections, due to its ubiquity and utility. Since the source code of the framework has leaked, we anticipate even further adoption of Cobalt Strike by all facets of threat actors.

We also anticipate that, despite various publications detailing detection methodologies, espionage-oriented actors are less likely to modify their server-side components. Threat actors engaged in state-sponsored espionage will use whatever tooling necessary to achieve their goals. If targeted organizations are unable to defend their network from tooling that has been disclosed, threat actors have little motivation to pursue new capabilities. Financially motivated actors using custom tooling, however, are very likely to respond to detections by either rebuilding their components (as was the case with BazarBackdoor and TrickBot actors) or introduce entirely new tooling (which FIN7 is known to do).

Due to these factors, it is important to implement security controls and mitigations against these malware families. While proactive detection of the command and control servers can help prevent incidents, defense-in-depth approaches are recommended to detect intrusion activity on the victim host, at the perimeter, and on the wire.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.