CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

March 15, 2022

2021 Malware and TTP Threat Landscape

Recorded Future®

The annual threat report surveys the threat landscape of 2021, summarizing a year of intelligence produced by Recorded Future's threat research team, Insikt Group. It draws from data on the Recorded Future® Platform, including open sources like media outlets and publicly available research from other security groups, as well as closed sources on the criminal underground, to analyze global trends, malware trends, and the top trending tactics, techniques, and procedures (TTPs) from 2021. The report will be of interest to anyone seeking a broad, holistic view of the cyber threat landscape in 2021.

Executive Summary

After major disruptive attacks and constant tool development throughout 2021, ransomware-related threats have been at the forefront of security teams' priority lists. Ransomware dominated as a major threat globally to organizations in several industry verticals. In late 2019 and throughout 2020, ransomware emerged as a major threat to larger organizations, which was considered "big game hunting" targeting. Throughout 2020 and into 2021, however, it evolved into a commoditized market, allowing for an increase in ransomware operators and more widespread attacks. Threat actors hired skilled individuals to develop functionalities within ransomware, rented ransomware out to affiliates, and purchased access to the networks of victim organizations from initial access brokers. In 2021, ransomware continued to be a successful business in the cybercriminal world, with Conti and LockBit leading the charge as the most prolific ransomware operations.

Ransomware groups relied on "double extortion" throughout 2020, which provides additional pressure on victims to pay their ransom by not only locking access to their systems but also threatening to leak or sell the stolen data unless the ransom is paid. In 2021, threat actors have shifted tactics and implemented"triple-extortion" techniques. These include the recruitment of insiders to breach corporate networks, contacting victims' customers to demand a ransom payment, threatening ransomware victims with distributed denial-of-service (DDoS) attacks, and targeting supply chains and managed service providers to amplify the effects of the attack. In addition, some ransomware groups began targeting Linux systems and added rapid vulnerability exploitation and zero-day vulnerabilities to their arsenal.

The dark web market for credential theft was very successful in 2021 and also contributed to ransomware attacks, as ransomware operators often use compromised credentials for initial access in attacks. Compromised credentials were regularly stolen using infostealers and advertised on dark web shops. These exposed passwords put networks at risk when corporate credentials were included in compromised logs or when employees reused passwords across personal and work accounts.

Alongside ransomware, malware and malicious tools such as Cobalt Strike evolved to become more difficult to detect and more dangerous when installed. We observed a continued trend of rapid vulnerability exploitation in malware attacks, especially with the late-2021 disclosure of what is widely considered one of the worst security flaws ever discovered, Log4Shell.

Lastly, in an investigation into the top MITRE ATT&CK TTPs throughout 2021, Insikt Group identified the top 5 techniques: T1486 (Data Encrypted for Impact), T1082 (System Information Discovery), T1055 (Process Injection), T1027 (Obfuscated Files or Information), T1005 (Data from Local System).

2021 Ransomware Landscape Overview

In 2021, ransomware operators conducted major attacks that affected high-profile victims including American food processing company JBS, and IT management company Kaseya. However, the most notable attack of the year targeted the US gas company Colonial Pipeline, with disruption of their operations heavily affecting gas distribution and pricing along the US East Coast. This attack demonstrated the massive consequences that can occur due to ransomware and was a turning point in the crackdown on ransomware from the US government and international law enforcement agencies.

New ransomware groups have continued to appear as cybercriminals observe the large profits that are made from operations against high-value targets. New threat actors almost exclusively are adhering to the data leaks model of double extortion, which provides additional pressure on victims to pay their ransom.

We have seen threat actors shifting tactics to target Linux systems, which increases the risk to organizations as Linux systems often host virtual machines and containers, both of which regularly host critical and potentially sensitive information. In addition, groups have demonstrated rapid vulnerability exploitation, as seen with the ProxyShell and Log4Shell vulnerabilities, and even exploited zero-day vulnerabilities as seen in the REvil ransomware attack on Kaseya. New tactics also involve recruitment of insiders to breach corporate networks, contacting victims' customers to demand a ransom payment, threatening ransomware victims with DDoS attacks, and targeting supply chains and managed service providers to amplify the effects of the attack.

Continued government and private sector intervention and pressure has successfully disrupted some ransomware groups. Several major ransomware groups have shut down operations, including Avaddon, REvil, DarkSide, and BlackMatter; however, after operations were shut down, we regularly saw affiliates who were associated with those groups shift to Conti and LockBit, which have contributed to their becoming the most active ransomware-as-a-service (RaaS) platforms this year.

Ransomware has proven costly to more than just the bottom lines of corporations throughout 2021. According to a lawsuit filed against Springhill Medical Center, the hospital fell victim to a ransomware attack, which ultimately led to the death of an infant. The lawsuit alleges that the disruption from the cyberattack on Springhill meant that critical data about the baby's elevated heart rate, information that could have enabled a faster delivery by caesarean section, was not available to doctors. While the hospital denies wrongdoing, this case represents the first reported death in the US linked to a ransomware attack, and it illustrates the legal, and more importantly, human costs that can occur from the disruptions caused by ransomware.

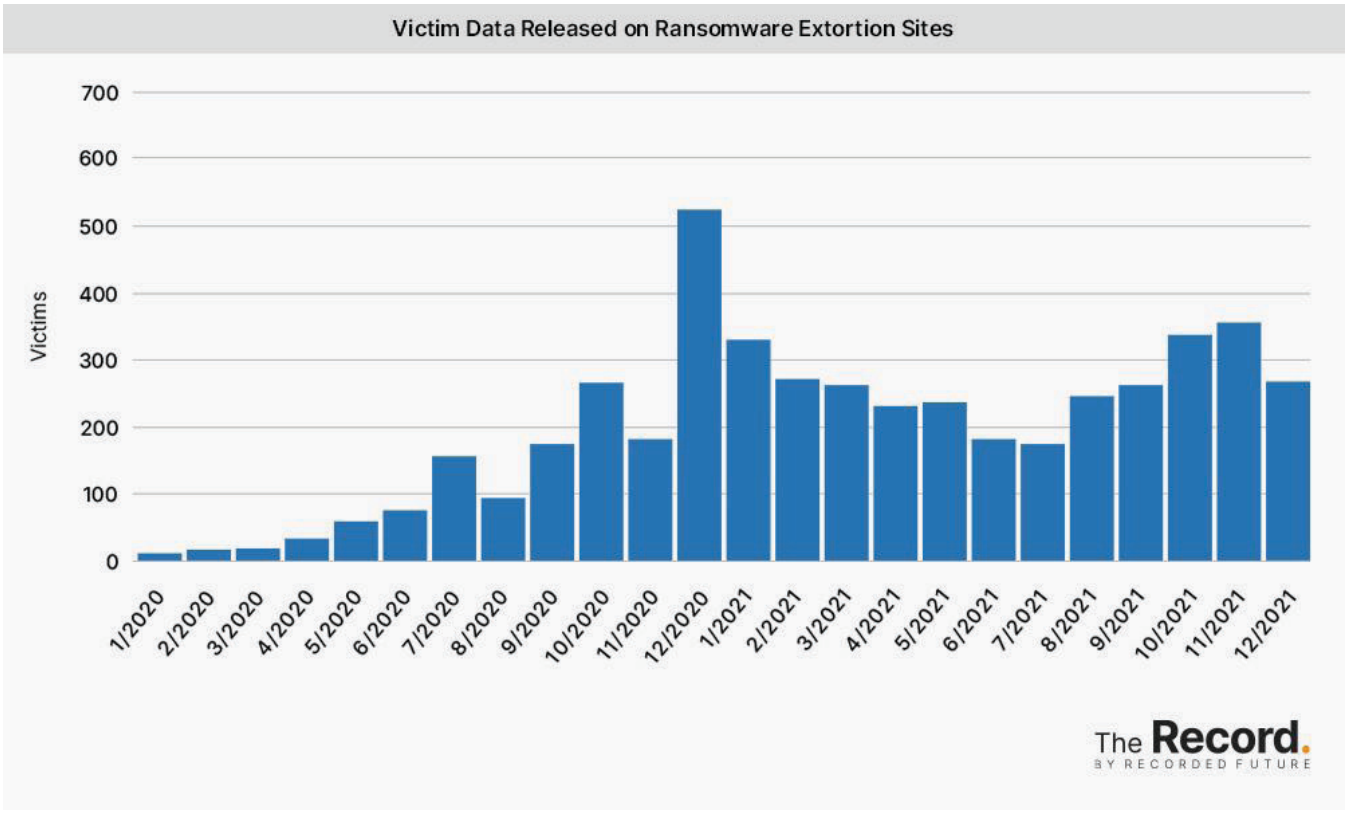

Figure 1: Volume of victims posted on extortion sites between 2020 and 2021 (Source: The Record)

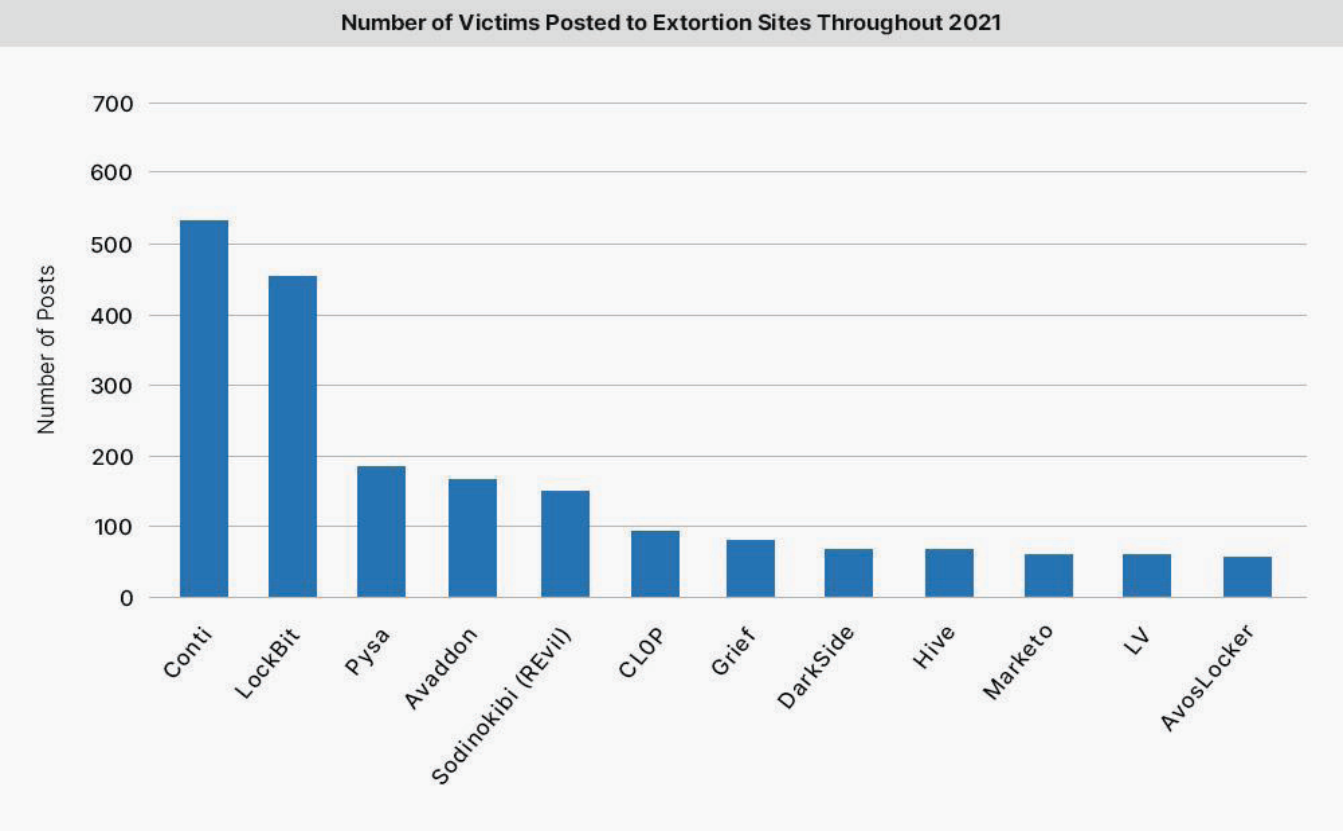

Figure 2: Number of victims posted to each ransomware operator's extortion site in 2021 (Source: Recorded Future)

Ransomware in 2021 at a Glance

Recorded Future tracked 58 different ransomware families that published 2,865 victims from 141 different countries to their extortion websites throughout.2021

When compared to the volume of victims listed on extortion sites between 2020 and 2021, the overall volume in 2021 increased by 106%.

According to Recorded Future data ,Conti ransomware published the most victims to their ransomware extortion website throughout ,2021 with 530 victims ,followed by LockBit with467 victims .Pysa ,Avaddon ,and REvil followed Conti and LockBit ,all with over 150 victims.

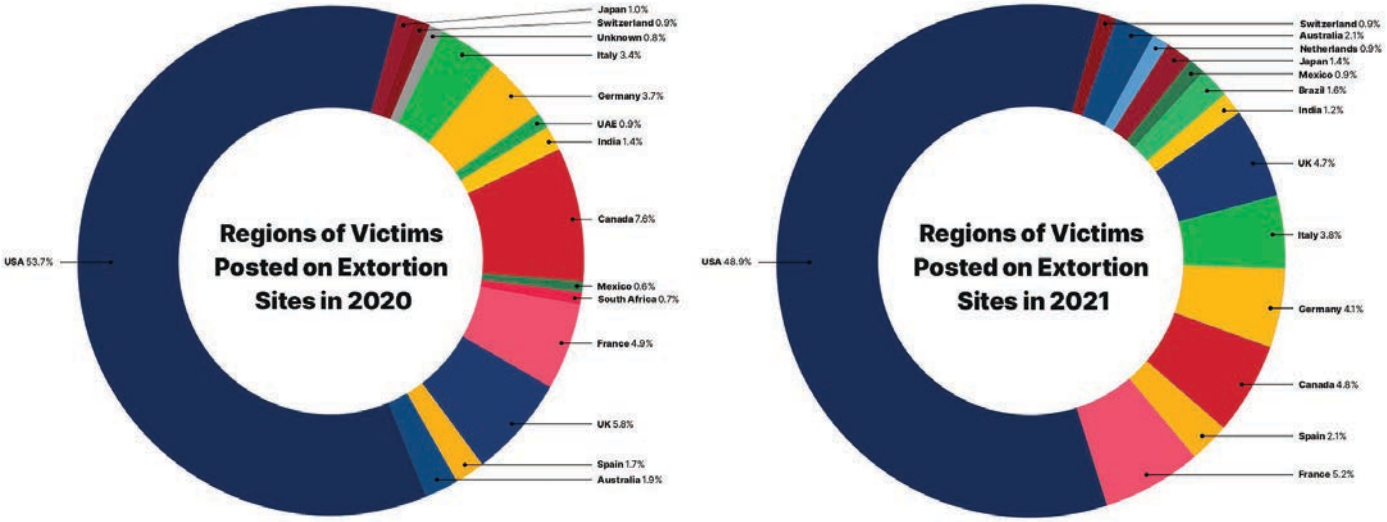

***Figure 3**: Regions of victims posted to extortion sites in 2020 and 2021 (Source: Recorded Future)*

Of the victims identified in 2020 by Recorded Future analysts:

- 53.7% were located in the US
- 7.6% in Canada
- 5.8% in UK
- 4.9% in France
- 3.7% in Germany
- 3.4 % in Italy

Of the victims identified in 2021 by Recorded Future analysts:

- 49% were located in the US
- 5.2% in France
- 4.8% in Canada
- 4.7% in the UK
- 4.1% in Germany
- 3.8% in Italy

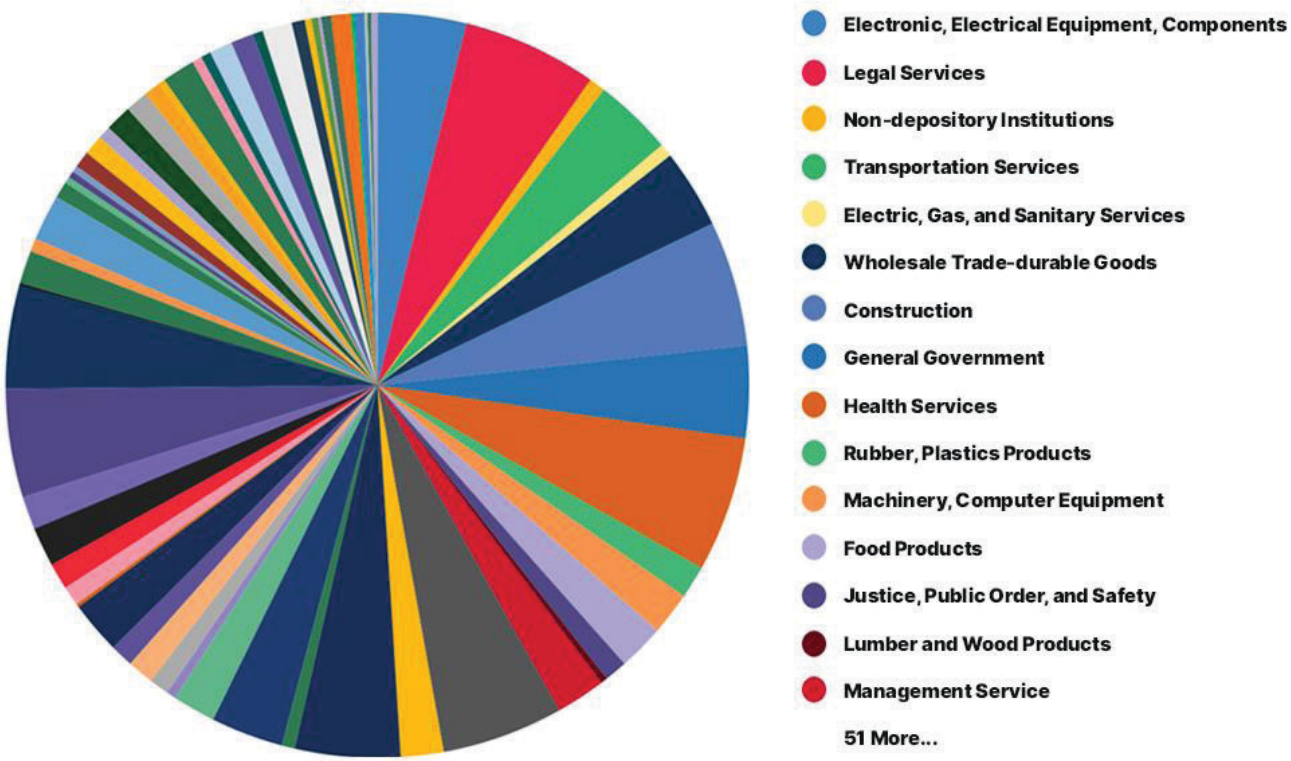

Figure 4: Industries targeted by ransomware operators in 2021 (Source: Recorded Future)

Throughout 2021, ransomware gained mainstream media attention for targeting critical infrastructure, specifically the attacks against Colonial Pipeline and JBS. However, in a review of data tracking ransomware attacks in 2021, Recorded Future analysts believe that ransomware operators and their affiliates are opportunistic by nature. They do not typically focus on specific industries or geographic regions, but rather select and pursue organizations based on accessibility, opportunity, and factors such as the type of data that has been accessed and exfiltrated along with the victim's ability to pay large ransom amounts (judged by company revenue). This wide range of industries affected by ransomware is illustrated by the array of colors for each affected industry, seen in Figure 4 above.

Ransom Demands and Payments

Ransomware demands and payments are difficult to track as they often happen on private channels .Reporting from Prodraft showed that ,as of mid-November ,2021 Conti ransomware had earned at least 25.5$ million USD from attacks and subsequent ransoms carried out within a-5 month period .However ,based on internal analysis conducted by Insikt Group derived from a variety of sources ,we believe that Conti has received more than 200$million USD since its inception in.2017

Considering the large ransoms paid to actors as a result of ransomware attacks, along with a reported $400 million worth of cryptocurrency stolen by North Korean hackers over the course of 2021, this is a massive transfer of wealth from corporate organizations to cyber criminal enterprises. This transfer of wealth will likely contribute to investments into retooling of infrastructure that will be used in attacks throughout 2022.

Using open-source data for the largest requested ransom demands throughout 2021 [1, 2] for public organizations, we found that **the average ransom demanded was 0.16% of the victim's annual revenue numbers**; while the number varied from 0.02% to 0.37%, the annual revenues identified are in the tens of billions of dollars, making the ransom demands large sums of money. While this number doesn't necessarily predict what the ransom demand may be, as other factors could influence this number such as the victim organization's prominence or the type of data compromised, it can help organizations estimate what a hypothetical ransom demand could look like. It should be noted that not all of the organizations listed in the table below paid the requested ransom.

Dark Web Exposure: Harvesting Credentials Using Infostealer Malware

The market for credential theft was successful in 2021 and contributed to ransomware attacks. While ransomware operators used several methods for initial access in attacks, compromised credentials were regularly exploited to obtain network access.

Compromised credentials are regularly advertised on dark web shops such as Genesis Store, 2easy Shop, Russian Market, and Amigos Market. In June 2021, Insikt Group confirmed that Amigos Market and Russian Market are connected as they were posting identical listings that contained the same timestamps, infostealer variants used, geographical locations of affected machines, and ISPs.

These shops advertise logs containing victim credentials harvested from victims infected with infostealers available in the criminal underground. Infostealer malware works as a remote access trojan (RAT) capable of stealing users' system information along with account login credentials, browser cookies, and autofill information. This information assists attackers in bypassing certain security protocols including multi-factor authentication (MFA). Stealers commonly used include RedLine, Vidar, Taurus, AZORult, Raccoon Stealer, and FickerStealer.

Cybercriminals can use compromised employee credentials to obtain unauthorized access to networks, conduct ransomware attacks, upload malware, exfiltrate data from the victim's host, and perform privilege escalation. While a vast majority of the compromised accounts are likely personal accounts, in some cases corporate credentials are included within these logs, which can present a significant risk to an organization's network. Additionally, because password reuse is common, threat actors can use personal account credentials against corporate networks, especially if MFA is not in place. And lastly, if an employee uses a personal computer infected with an infostealer for work, their information could be compromised and used to illegally access and exfiltrate corporate data.

This was evident in the DarkSide ransomware attack on Colonial Pipeline in May 2021 that led to the disruption of fuel distribution across the East Coast of the US. According to a report from June 4, 2021, incident responders confirmed that attackers were able to remotely access Colonial Pipeline's network using a compromised password to a VPN account that was no longer active.

According to investigators, it is unclear how DarkSide obtained the password, but they did confirm that the password was included inside of a collection of leaked passwords on the dark web, and it is possible that an employee used the password on a separate account external to Colonial Pipeline that was compromised. They also confirmed that they did not identify any evidence of phishing attacks targeting the employee.

Victim	Ransomware	Estimated Annual Revenue	Payments and Requested Ransoms	Percent of Ransom Demand Compared to Annual Revenue
Acer	REvil	277$billion	50$million	0.018
Brenntag	DarkSide	13.4$billion	7.5$million	0.056
CNA Financial Corp	Phoenix CryptoLocker	10.8$billion	40$million	0.37
Colonial Pipeline Company	DarkSide	1.32$billion	4.4$million	0.33
JBS	REvil	53$billion	11$million	0.02

Trending Malware TTPs

Recorded Future tracks developments in TTPs associated with malware or cyberattacks in our TTP Instance notes. In 2021, the malware that appeared most in these notes, which accounted for 6% of the notes, was Cobalt Strike. This was consistent with our observations this year about the predominance of Cobalt Strike in logs of C2 infrastructure. Both security researchers and criminals released several new versions of Cobalt Strike Beacon Object Files (BOFs), with new functionality including exploitation of Active Directory objects, DNS traffic masking, generation of random C2 profiles, domain borrowing, development directly in a .NET environment, Blowfish Cipher encryption, access to a Mimikatz Kit, Windows Firewall manipulation, and victim DLL file enumeration.

Altogether, these updates make Cobalt Strike Beacons more difficult to detect, and the increase in functionalities increases the breadth of malicious actions threat actors can perform. Recorded Future published research in 2019 about how to detect rogue Cobalt Strike servers, and many of the recommendations in that report hold true today. Insikt Group also published research in 2021 about Cobalt Strike use by threat actors and ensuing network and host-based detection opportunities.

Other types of malware received updates throughout 2021 as well. These updates included new user interfaces (such as for 365-stealer), support for exploiting newly disclosed vulnerabilities (such as for PrintNightmare by Mimikatz), and improvements in evading detection (such as for Lilith Botnet and Qakbot).

Common functionality across these new malware variants included credential stealing, cryptocurrency mining, privilege escalation, and masquerading as benign files or processes. We observed several updates or advertisements targeting Microsoft products, primarily for use as an initial access vector or evasion techniques for security tools. These included new TTPs for malicious Office documents and bypasses for Windows User Account Control (UAC) and Antimalware Scan Interface (AMSI).

Trending TTPs

According to Recorded Future data, the top 5 trending MITRE ATT&CK techniques in 2021 were T1486 (Data Encrypted for Impact), T1082 (System Information Discovery), T1055 (Process Injection), T1027 (Obfuscated Files or Information), and T1005 (Data from Local System). These techniques span across 5 stages of an attack: Discovery, Privilege Escalation, Defense Evasion, Collection, and Impact; 2 of the techniques are classified under Defense Evasion.

TTP	Details
T1486 (Data Encrypted for Impact)	Data encrypted for impact is our top technique for 2021 due to a high volume of ransomware attacks throughout the year.
T1082 (System Information Discovery)	System information discovery occurs when a threat actor attempts to get detailed information about the operating system and hardware. System information discovery is commonly performed by various malware to gather information about an infected device. Insikt Group has observed it in use by low-level and sophisticated actors alike throughout 2021.
T1055 (Process Injection)	Process injection involves running custom code within the address space of another process. Process injection has been a popular technique because of its defense evasion benefits (disguising malicious behavior as legitimate processes). Throughout 2021, we observed this technique used alongside several shellcode loaders and droppers.

TTP	Details
T1027 (Obfuscated Files or Information)	Obfuscated files or information is a technique where adversaries attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and networks to evade defenses. We observed attackers using this technique to compress, archive, or encrypt payloads in order to avoid detection throughout the year. Adversaries commonly used compressed or archived scripts, such as PowerShell and JavaScript.
T1005 (Data from Local System)	Data from local systems was continually used by ransomware groups that operate extortion websites throughout the year, as the threat actors will often search for and exfiltrate data prior to encryption. The threat actors then would use this data to extort their victims into paying ransom demands by threatening to leak the stolen data.

Similar to Insikt Group's 2019 and 2020 MITRE ATT&CK tactic and technique findings, Defense Evasion techniques continue to prevail for the third year in a row. When compared to 2020's top 6 MITRE ATT&CK technique list, T1082 (System Information Discovery), T1055 (Process Injection), and T1027 (Obfuscated Files or Information) persisted as prominent techniques used by malware over the course of the year.

While not in the top 5 techniques overall, based on Recorded Future data, the top initial access vectors throughout 2021 were T1190 (Exploit Public-Facing Application) and T1566.001 (Spearphishing Attachment).

Outlook

The diverse and evolving TTPs used by malware groups, and specifically ransomware operators, demonstrate the pressing need for a defense-in-depth strategy. This should include ensuring logging is positioned across an organization's network to detect anomalous activity, building a robust and efficient vulnerability management program to prioritize vulnerability patching, implementing Hunting Packages to hunt for known malicious behaviors, and integrating threat intelligence into preexisting security technologies to aid in triaging alerts. In addition, organizations should implement a structured and detailed employee security training program as employees are often the first line of defense, especially when it comes to preventing credential exploitation.

As long as the ransomware market continues to prove profitable, ransomware will continue to remain a significant threat to public and private entities throughout the year. We expect ransomware operators to continue to rely heavily on compromised passwords, vulnerability exploitation, and malware deployment for initial access to networks, although as security teams improve their patch management and attack surface, these resources for initial infection could diminish for attackers. Additionally, we expect Cobalt Strike to continue to be a regularly used tool for C2 communications to facilitate attacks, including ransomware deployment.

While ransomware will continue to target organizations worldwide, 2021 saw unprecedented global law enforcement action taken against ransomware groups. The 30-nation ransomware task force led by the US appears to be seeing early success with almost weekly announcements against ransomware groups, and in October 2021, the Deputy Attorney General of the US, Lisa Monaco, announced the launch of a National Cryptocurrency Enforcement Team at the Department of Justice to pursue criminals who target cryptocurrency marketplaces and use digital coins to launder money. Most recently, on January 14, 2022, the Russian Federal Security Service (FSB) announced that it has raided and shut down the operations of the REvil ransomware gang.

It is still too early to determine whether government intervention has led to a reduction in ransomware attacks, but there are some early indications that the combination of arrests, cryptocurrency exchange sanctions, and cryptocurrency seizures may be slowing down the number of ransomware attacks in some sectors and geographic areas. Alongside government intervention, Recorded Future's Allan Liska argues that there may be other factors contributing to a potential decline in attacks. Cyber insurance companies have begun requiring that policyholders have more stringent cybersecurity protections in place before they will renew a policy and, according to Gartner, companies spent 12% more on cybersecurity in 2021. With these defensive strategies, cyber threat groups, and especially ransomware operators, will likely continue to innovate on avoiding detections to facilitate attacks.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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