2021 Year in Review

Christopher “Tophs” Elisan
Javier Botella
Nicki “Nytemare” Copeland
Yiting Yu

Table of Contents

A Letter From PolySwarm's CEO 3

Predictions for 2022 4

Most Prolific Malware Families 5

- 2021's TRENDING MALWARE FAMILIES 5

Top Malware Families to Watch in 2022 7

Targeting by Vertical 8

Regional Highlights and Threat Actor Activity 9

- MENA 10
- APAC 13
- AMERICAS 16

2021 News Highlights 17

- Significant Ransomware Attacks 17
- Emerging Malware Threats 17
- TTPs 17
- The Fight Against Ransomware 18
- Arrests 18

Story of the Year: Apache Log4j Vulnerability (CVE-2021-44228) 19

Appendix A: Growing List of PolySwarm Ransomware Families Tracked 20

Appendix B: Sample IOCs 21

A Letter From PolySwarm's CEO

Early in 2021, PolySwarm's threat intelligence and development teams made many predictions about the types and scope of malware we'd see (e.g. cloud targeted crypto miners over ransomware). As our platform of 50+ engine partners and multiple sandboxes processed and convicted millions of malicious samples and URLs, it became clear that 2021 was the year of ransomware and its delivery systems. High profile ransomware stories, like Colonial Pipeline, confirmed this shift and provided ample real-world anecdotes of how organized and industrialized the underground economy has become. This was especially well illustrated in how quickly the details of the Log4j vulnerability spread in underground forums, with multiple actors discussing and sharing exploits to fully take advantage of the vulnerability.

In this report, we detail our analysts' take on the 2021 trends observed across our dataset. Along the way, our team got to compare their 2021 predictions with the reality of our dataset. We hope you enjoy reading as much as our team enjoyed validating (and invalidating) each other's predictions!

– Steve Bassi
CEO of PolySwarm

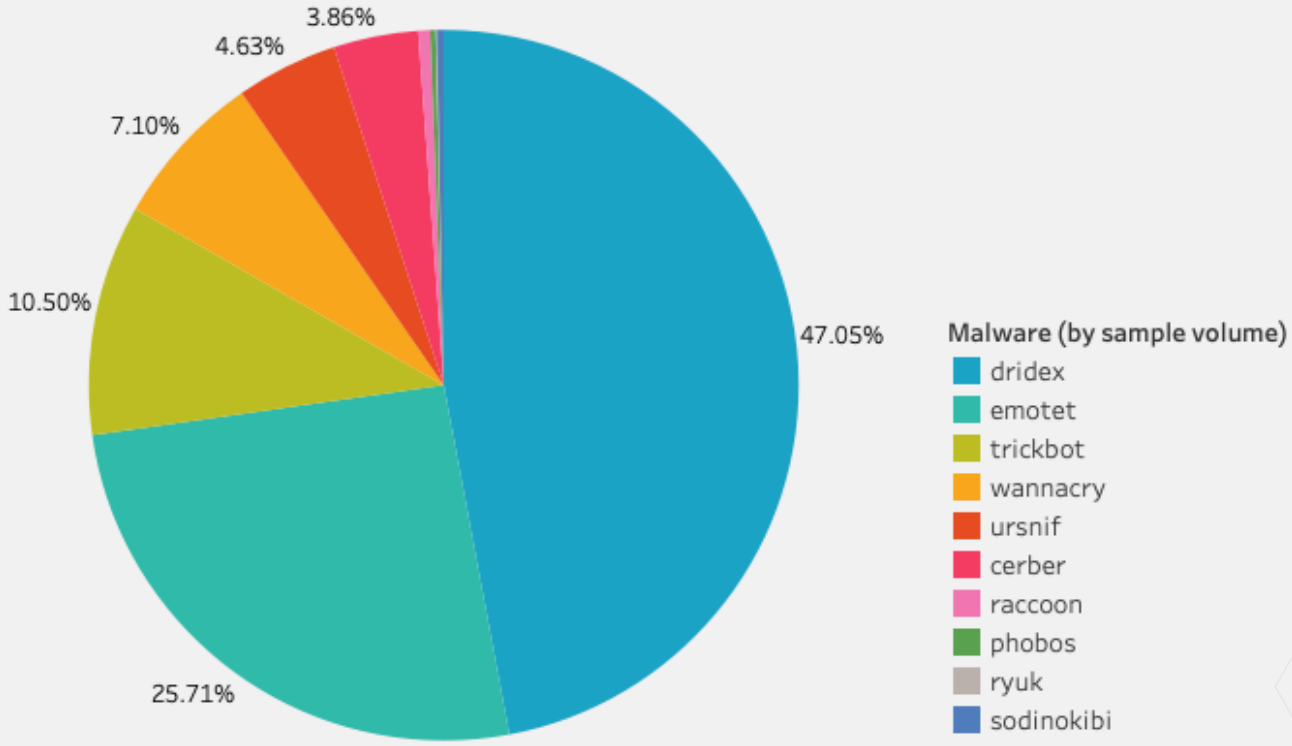
Predictions for 2022

- Threat actors will continue to evolve ransomware extortion tactics, leaving victims in a desperate situation and more willing to pay to recover files or to prevent operations disruption and reputational damage.
- Supply chain attacks involving ransomware will continue to escalate.
- More malware and ransomware variants targeting Linux systems will emerge given the Linux server's dominance in SaaS applications that hold private customer data.
- Threat actors will continue to create exploits targeting the Log4j vulnerability.
- Threat actors will conduct more tailored attacks, using thorough reconnaissance on potential targets in order to determine the most stealthy and most devastating methods for attacking those targets.
- Based on the objectives outlined in China's current Five Year Plan, which drives its national growth goals as well as its intelligence collection requirements, our analysts assess a high likelihood that Chinese state sponsored threat actors will focus on targeting the manufacturing, technology, and green energy verticals. Additionally, we predict an increase in espionage-focused attacks against political and economic targets in the US and Taiwan.
- Due to ongoing tensions between Russia and Ukraine, we assess a sharp increase of deniable, but state sponsored espionage campaigns.
- Continuation or escalation of the COVID-19 pandemic will continue to serve as a backdrop for threat actor activity, with threat actors using COVID-19 themed phishing lures and targeting entities in the healthcare and biomedical research verticals.
- Threat actors will continue to seek novel ways to target 5G infrastructure, particularly as the use of 5G technologies grows.
- Ransomware gang cartels will continue to evolve in response to attempts by governments worldwide to stop ransom payment. Additionally, threat actors will continue to leverage affiliate programs to infect previously compromised networks or to entice insiders to allow access for a cut of the profits.

Most Prolific Malware Families

At PolySwarm, we track over 85 major malware families. A list of these families can be found in Appendix A. The top 10 most submitted malware families for 2021 were a combination of ransomware and banking trojans. They are represented in the chart below:

2021's TRENDING MALWARE FAMILIES



What makes each of these malware families significant? Here is a bit of background on each of our top 10 malware families.

Dridex

Dridex, also known as Bugat and Cridex, is a banking trojan, a malware used to steal banking credentials. Dridex targets Windows systems. Dridex has been attributed to the group known as Evil Corp, a financially motivated threat actor group with a Russian nexus. Dridex was observed being spread by a new phishing email campaign in late 2021.

Emotet

The Emotet banking trojan, first seen in the wild in 2014, was once considered the "world's most dangerous malware" and had an elaborate infrastructure. The binary is typically spread via a phishing email containing a malicious attachment or a link to a malicious Word attachment. Following an infection, it spreads laterally via the SMB Admin$ share, making it one of the most resilient malware families. Emotet is also polymorphic, meaning the binary changes with each infection, making detection more difficult. Although authorities took down the Emotet botnet in early 2021 and seemingly eradicated the virus from victim machines, Emotet activity has once again been observed in the wild

TrickBot

TrickBot, active since 2016, is an advanced banking trojan targeting Windows systems and spreads primarily through spearphishing campaigns. Trickbot's ability to survive takedowns makes it a well worn infection vector for ransomware gangs. 2021's banner year for ransomware would not be possible without commodity delivery systems like Trickbot, which was high up in PolySwarm's dataset. The latest ransomware to use Trickbot as its infection vector is Diavol.

WannaCry

Wannacry is a ransomware containing a worm component that exploits vulnerabilities in the Windows SMBv1 server. WannaCry first emerged in 2017, leveraging the Eternal Blue exploit allegedly developed by the NSA. The initial attack compromised around 230,000 machines. WannaCry highlighted the dangers of a ransomware attack affecting healthcare vertical entities, as it compromised many of the UK's NHS systems. Threat actors took advantage of the COVID-19 pandemic to resurrect WannaCry. Despite WannaCry being a relatively old ransomware, it is still active because some organizations have failed to patch the EternalBlue exploit the malware uses to compromise Windows machines and propagate itself. The new variant seen in 2021 also had the kill switch removed, which had thwarted the early WannaCry variants.

Ursnif

Ursnif, also known as Gozi and Dreambot, is a widely used banking trojan that also has backdoor, spyware, and file injector components. More recent versions of Ursnif are typically spread via a phishing email containing a malicious MS Word document. The financially motivated threat actor group TA544 was observed targeting Italian organizations with Ursnif in late 2021.

Cerber

Cerber is ransomware-as-a-service (RaaS) operating with an affiliate program. It is most often delivered via phishing emails, infected websites, and malvertising and targets both Windows and Linux. Cerber drops both a ransom note and an audio file to address the victim. In late 2021, a new Cerber campaign emerged leveraging CVE-2021-26084 and CVE-2021-22205, targeting Confluence and GitLab servers.

Raccoon

Raccoon infostealer, also known as Racealer or Mohazo, is a relatively unsophisticated malware as a service (MaaS) written in C/C++ and targeting Windows systems. It was first seen in the wild in late 2019. Raccoon is often used to steal login credentials, credit card information, cryptocurrency wallets, and browser information. In 2021, the threat actors behind Raccoon announced a new module called Racoon Clipper in underground forums. Racoon Clipper is available as an add-on for $50 USD and targets Bitcoin, Dogecoin, Ethereum, Litecoin, and Monero cryptocurrency wallets.

REvil

REvil also known as Sodinokibi, is ransomware as a service (RaaS) operated by the REvil ransomware gang. While several key members of the REvil ransomware gang were allegedly arrested in late 2021 and early 2022, the group was very active prior to law enforcement intervention. However, according to recent industry reporting, the REvil implant still remains active, indicating the group has not entirely ceased operations. As with other arrests made in the past, the group is likely to survive as long as there are existing affiliates willing to spread the ransomware; and the main ransomware code-base and campaign-supporting infrastructure remains intact.

Phobos

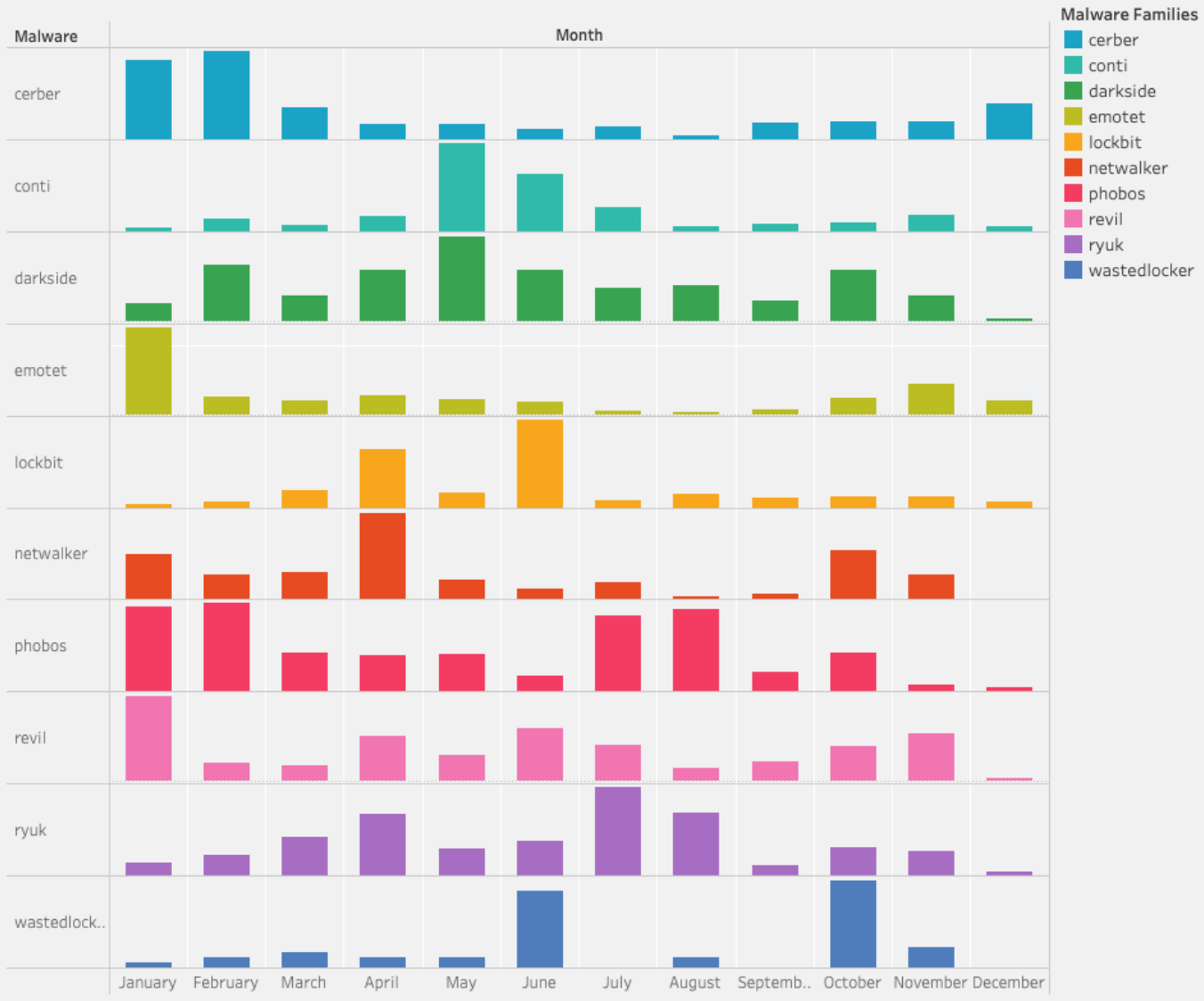
Phobos ransomware was first observed in 2019 and is related to the Dharma malware family. It targets Windows systems and is typically distributed via hacked RDP connections. In mid-2021, the average Phobos ransom payment was around $54,700.

Ryuk

Ryuk ransomware, known for its “big game hunting,” targets organizations with high ransom demand. Industry researchers have attributed Ryuk to a financially motivated, Eastern European, threat actor group dubbed Fin12. In 2021, a new Ryuk variant featuring worm-like capabilities to spread via RPC was observed in the wild.

Top Malware Families to Watch in 2022

Some of our most active malware families of 2021 are shown below, based on month over month trending data. Our analysts predict these will be among the top malware families to watch in 2022.



Cerber is described in the previous section.

Conti is attributed to an Eastern European threat actor known as Wizard Spider. A newer Conti variant seen in the wild has the ability to destroy backups, which are obviously a key strategy used by victims to avoid ransom demands. In late 2021, Conti focused on victims using Veeam backup software, which easily allows privilege escalation to local Administrator permissions on a target machine, and allows an attacker to move laterally.

DarkSide is a ransomware that is configurable to target files on fixed, removable disks, or network shares. While the threat actor group behind this ransomware reportedly ceased activity in mid-2021, DarkSide samples continued to appear in the wild through the end of 2021. This likely indicates the threat actors responsible for DarkSide continue to operate in some capacity. Some of the actors associated with DarkSide reportedly rebranded as BlackMatter. Based on the group's previous rebranding, our analysts assess a high likelihood of the remnant of this threat actor group reemerging under a different name and with a new ransomware variant in 2022.

Emotet is described in the previous section.

LockBit ransomware is RaaS that uses a quick encryption process to encrypt a victim's files in demand for a ransom.

Netwalker is ransomware-as-a-service, meaning affiliates rent the code for a commission on victim payout. It has resulted in at least one death due to targeting healthcare facilities. Industry researchers have attributed Netwalker to an Eastern Europe based threat actor group known as Circus Spider.

Phobos is described in the previous section.

REvil is described in the previous section.

Ryuk is described in the previous section.

WastedLocker is operated by EvilCorp, the group also known for the Dridex banking trojan. WastedLocker uses a JavaScript-based framework known as SocGholish to trick victims into infecting themselves via fake updates.

SAMPLES OF ALL MALWARE FAMILIES MENTIONED IN THIS REPORT ARE AVAILABLE ON OUR PORTAL.

Targeting by Vertical

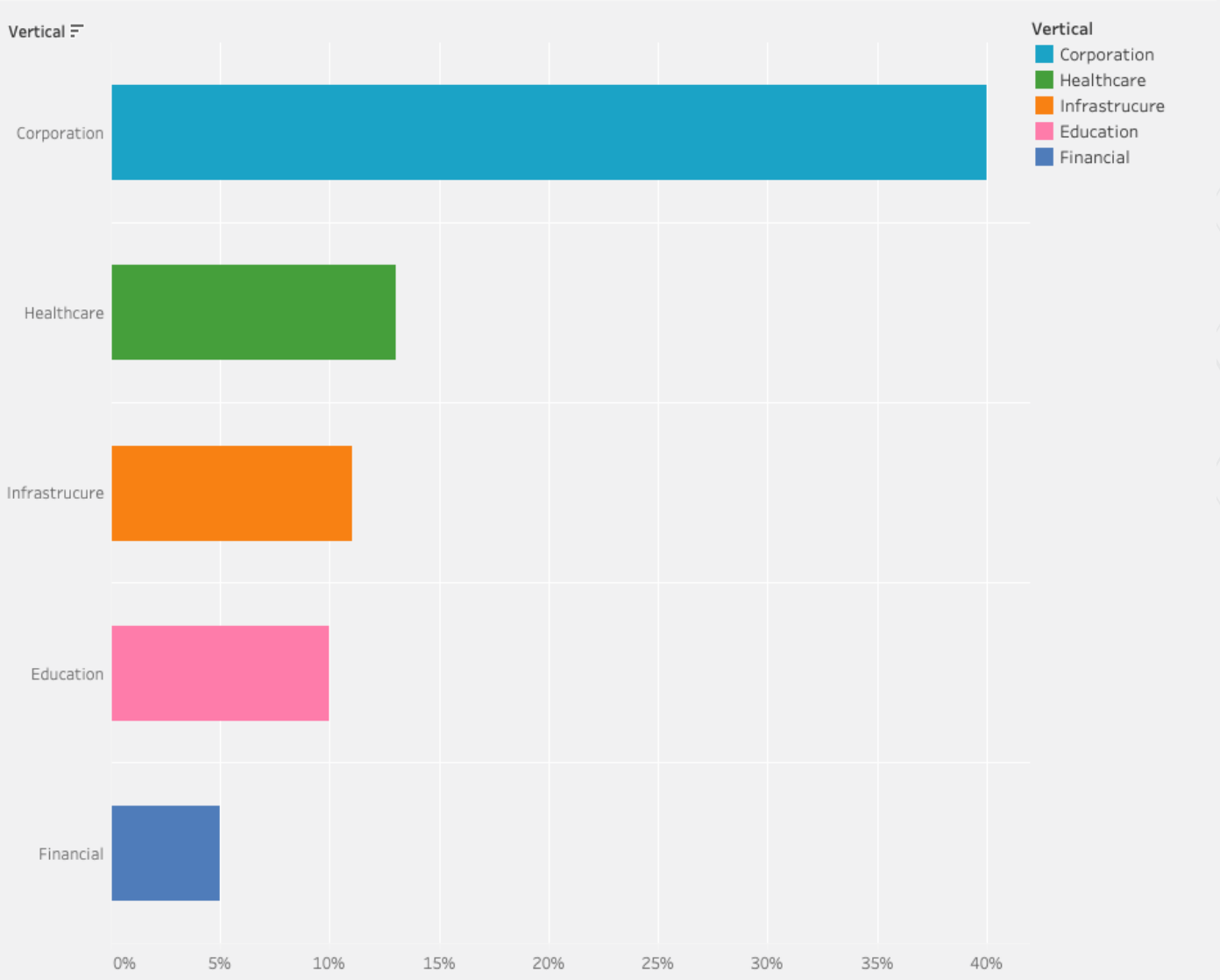
In 2021, corporations, healthcare, infrastructure, education, and financial were the verticals most targeted by ransomware.

The COVID-19 pandemic had a significant impact on targets chosen. Many corporations expanded their work from home programs, and schools switched to remote classrooms, broadening the threat landscape associated with those verticals. And the healthcare vertical was a prime target due to the increased importance of prompt medical care.

Osterman Research found that global enterprises with multiple subsidiaries are more likely to experience cybersecurity threats, due to the difficulty of implementing consistent security controls. Inconsistent security controls across subsidiaries ultimately make the parent company (and their bottom line) vulnerable to multiple attacks from business email compromise to ransomware.

The FBI issued a Private Industry Notification stating ransomware threat actors have begun targeting organizations undergoing significant financial transactions, such as mergers and acquisitions, as it obviously increases a victim's motivation to pay up.

RANSOMWARE TARGETING BY VERTICAL



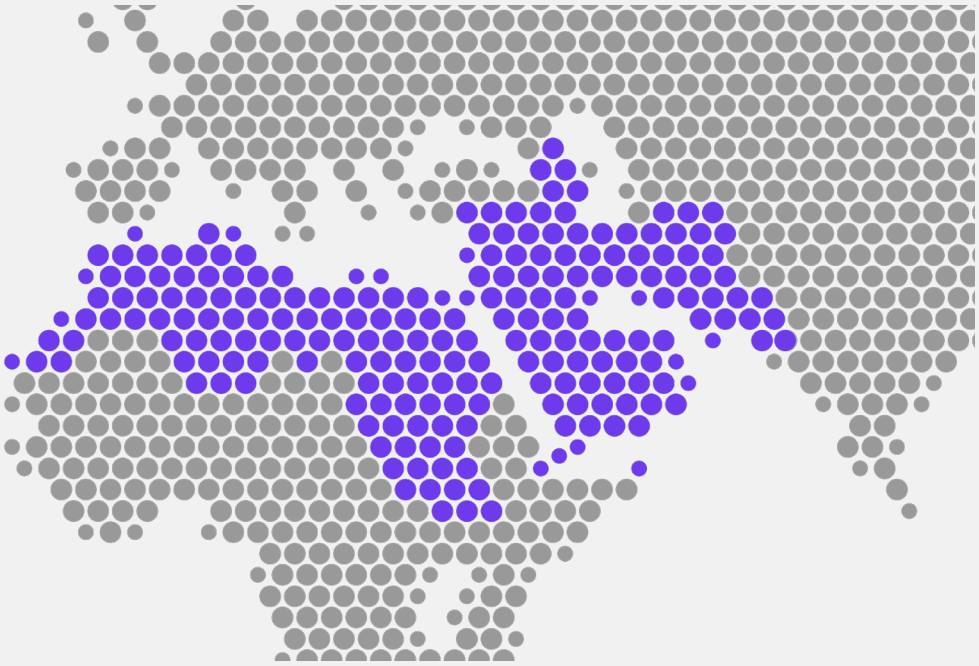
Regional Highlights and Threat Actor Activity

At PolySwarm, we track certain malware families by associated target and production languages and regions found in the malicious artifact. At a high level, this information comes from multiple metadata fields. These data fields can include locale of tooling, locale of Windows executables, and written languages found in malicious dropper documents. The language derived from these fields is typically the language of targeting and not the language of origin. This metadata can be used to create visual representations of samples containing a particular language.

We currently track four Middle East and North Africa (MENA) languages, and eight APAC languages. Our researchers also conduct both original and OSINT research to track threat actor activity in all regions. A small selection of hashes of APT malware samples we have is provided in Appendix B.

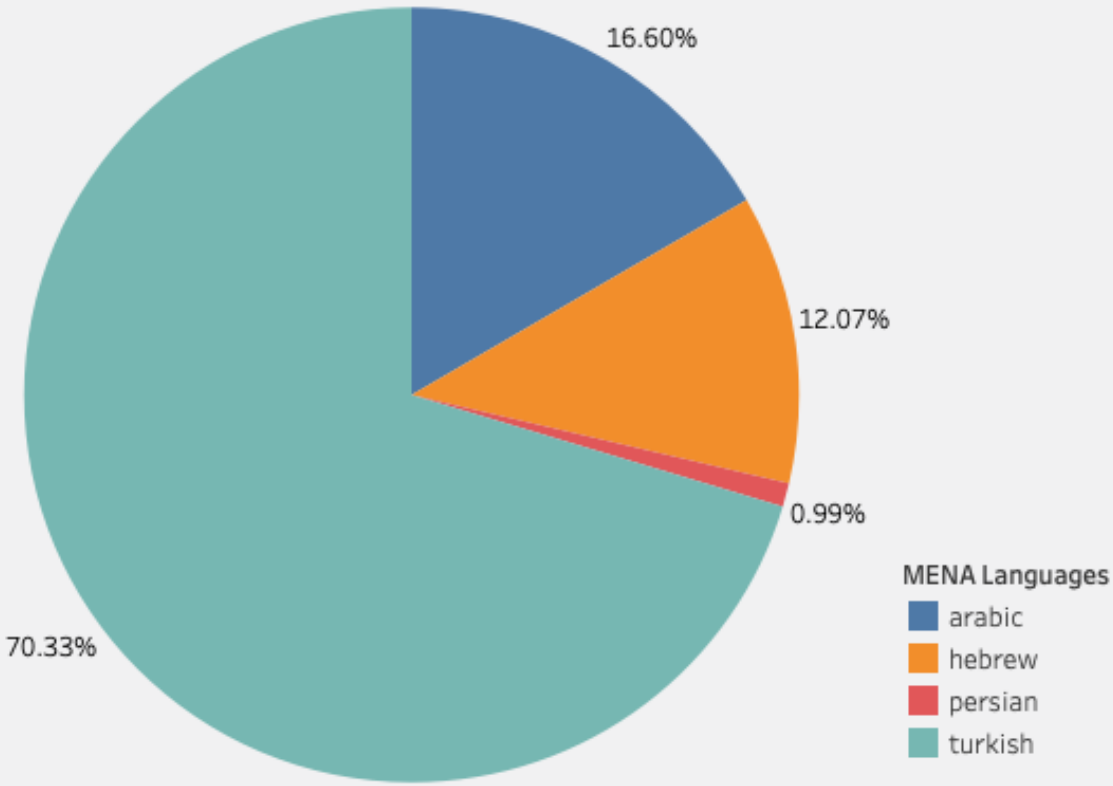
Below is a representation of the most active languages tagged for the languages we track, as well as regional highlights for threat actor activity in 2021.

MENA



The languages PolySwarm tracks in the MENA region include Arabic, Hebrew, Persian, and Turkish.

MENA SAMPLES BY LANGUAGES



This year, Turkish was the most prevalent tracked language in malware samples from the MENA. According to industry reporting, Turkey's threat landscape is ripe for malware due to its high internet penetration and relatively low security. This trend follows an increase in malware targeting organizations based in Turkey back in 2020.

- **StrongPity** (Turkey) used new TTPs including Android malware in and a new three-stage attack disguised by a Notepad++ installation.

Iranian state sponsored threat actors were particularly active in 2021, primarily targeting Israel, UAE, and Saudi Arabia. We expect an increase in samples written for Hebrew and Arabic language targets over the next few months based on the reported use of ransomware by six Iranian nexus threat actor groups.

Ongoing cyber tensions between Israel and Iran affected civilians and had an impact on kinetic entities in 2021. Those affected included fuel distribution systems in Iran. Iranians were stranded or had to wait in line for hours to obtain gas, leaving many people unable to continue daily operations. Digital billboards were hacked displaying the message "Khamenei, where is my gasoline?" and the phone number of the office of Iran's supreme leader, Ayatollah Ali Khamenei. It took weeks for affected entities to return to full operational capacity. An increase Persian language malware samples we observed in late November may reflect an escalation in this ongoing cyber dispute.

Iranian threat actors were responsible for multiple espionage campaigns.

- **Hexane** (Iran) reportedly attacked an IT company in Israel and targeted ISPs and telecommunications organizations in Israel, Morocco, Tunisia, and Saudi Arabia. They also targeted a ministry of foreign affairs in Africa.
- **Static Kitten** (Iran) was responsible for multiple campaigns, including counterespionage operations targeting UAE and Kuwait government agencies, the Operation Earth Vetala spearphishing campaign, and an espionage campaign targeting telecommunications organizations in the Middle East and Asia.
- **Charming Kitten** (Iran) masqueraded as British scholars to covertly target individuals of intelligence interest to the Iranian government. In December, Charming Kitten was observed leveraging the Log4j vulnerability to drop malware.
- **OilRig** (Iran) emerged with a new campaign targeting organizations in Lebanon and new TTPs including the SideTwist backdoor.

In Europe, some of the most active threat actors were Eastern European based ransomware gangs including **REvil**, **Evil Corp**, **Wizard Spider** (Conti), and **CLOP**.

- **Evil Corp** (Russia) successfully targeted multiple companies with ransomware including CNA insurance company, Sinclair Broadcasting, Forward Air, and Olympus.
- **DoppelPaymer** (Russia) reportedly targeted multiple entities with ransomware including Kia Motors, the Illinois Attorney General's office, and the NRA. Industry researchers observed the group using a quadruple extortion technique.
- **Wizard Spider** (Russia) reportedly targeted numerous organizations with ransomware including FatFace clothing, the Scottish Environmental Protection Agency, 700 Spanish government labor agency offices, the Florida school system, Volue, Ireland's Department of Health, New Zealand hospitals, Exagrid, the City of Liege in Belgium, Tulsa Police, a Nokia subsidiary, JVC Kenwood, Sandhills Machinery, Graff celebrity jewelry house, Australian government assets, Nordic Choice Hotels, CS Energy in Australia, McMenamins Breweries, and Shutterfly. The threat actor was also observed creating a fake movie site named BravoMovies to target victims using BazaLoader.

- Financially motivated threat actor **TA-505** (Russia) began using new TTPs including KiXtart Loader, MirrorBlast loader, and a new FlawedGrace variant. They conducted campaigns targeting entities in the US, Canada, Germany, and Austria.
- REvil ransomware gang (Russia) reportedly targeted Dairy Farm, Acer, Asteelflash, Pierre Fabre, Brazil's Rio Grande do Sul court system, JBS, Fujifilm, US nuclear weapons contractor Sol Oriens, Grupo Fleury, MasMovil, Fimmick, and Kaseya. The group temporarily ceased operations in mid-2021 after their website was shut down but resumed activity in September. The group also threatened to call the business partners of victim organizations as a new form of extortion. The group used new TTPs including REvil ransomware variants with a new Windows Safe Mode encryption mode and variants with a backdoor to cheat affiliates. Several key individuals associated with the REvil ransomware gang were arrested in late 2021 and early 2022.
- Carbon Spider (BlackMatter) (Ukraine) had money and servers confiscated by government authorities. In November, the group announced it was ceasing operations.

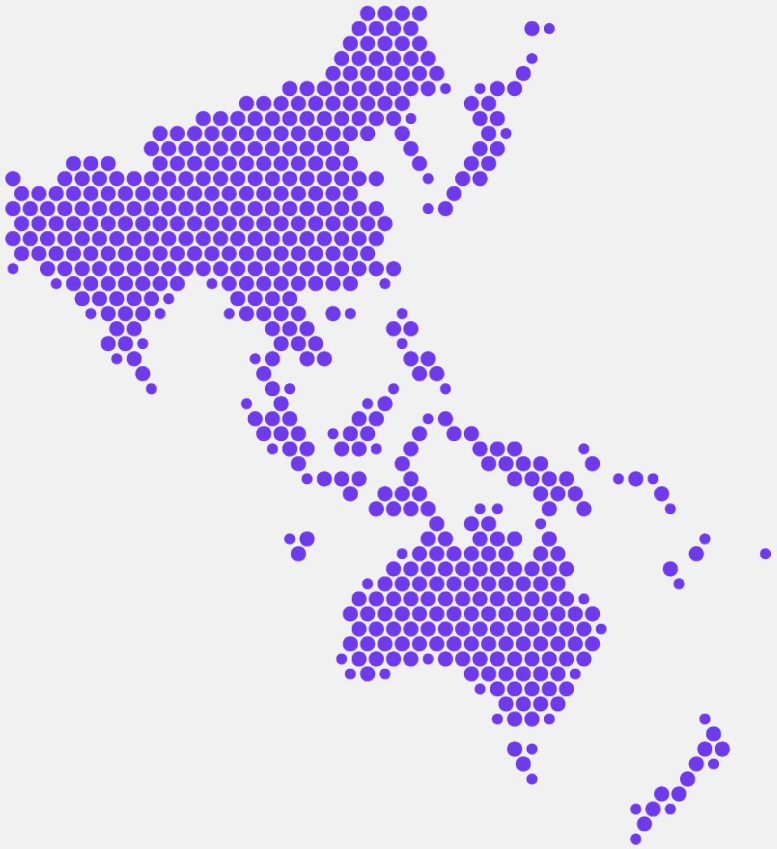
State sponsored Russian nexus threat actor groups were also very active.

- **Cozy Bear** (Russia) was one of the most active Russian threat actor groups in 2021. Industry researchers attributed the 2020 SolarWinds hack to Cozy Bear, and in 2021, the group continued its activity with various espionage campaigns targeting governments and businesses worldwide.
- **Venomous Bear** (Russia) was observed using new TTPs including a new backdoor to maintain persistence and a new loader IronNetInjector.
- **Fancy Bear** (Russia) began using new TTPs including the SkinnyBoy malware implant. They also targeted Gmail users via spearphishing with unknown motivation.
- **Primitive Bear** (Russia) was allegedly observed conducting information operations to promote growing hostility between Russia and Ukraine.

Other threat actors in the region conducted new campaigns and adopted new TTPs.

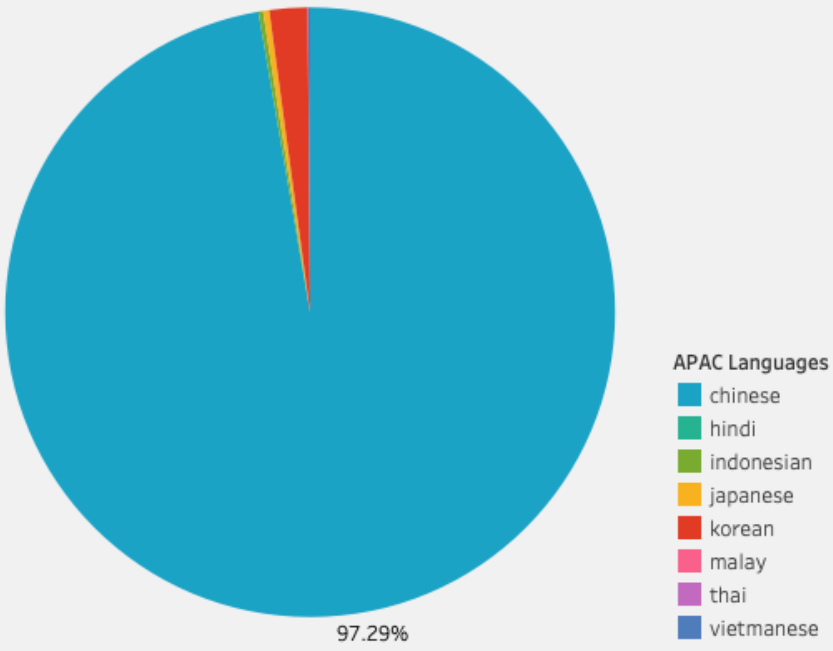
- In Early 2021, the threat actor group known as **Gaza Cyber Gang** (Gaza region) ran espionage campaigns against various government targets in the Middle East.

APAC



The languages PolySwarm tracks in the APAC region include Chinese, Hindi, Indonesian, Japanese, Korean, Malay, Thai, and Vietnamese.

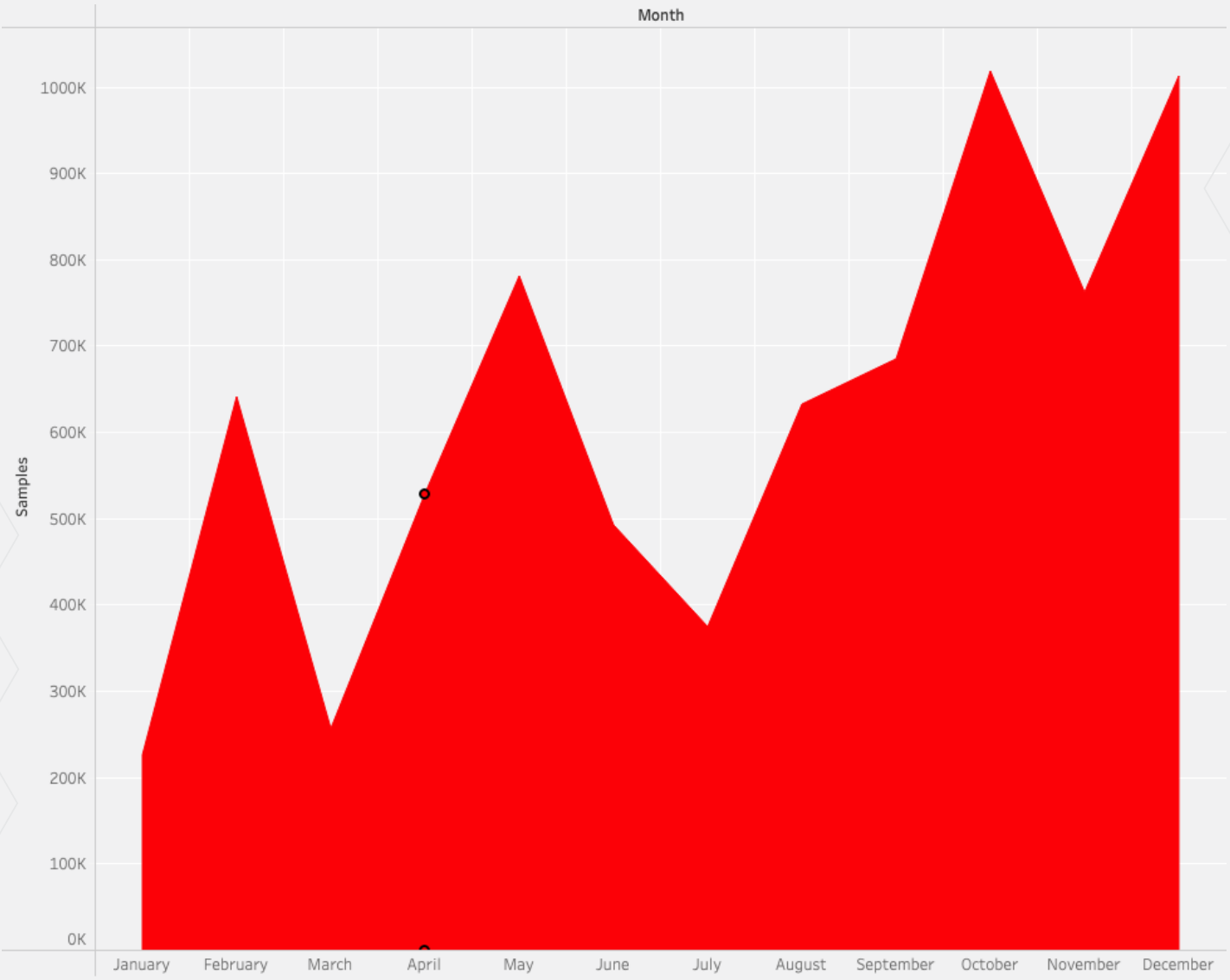
APAC SAMPLES BY LANGUAGES



In the APAC region, the most prevalent language derived from metadata in our malware samples was Chinese. This is no surprise, due to the ongoing operations of both state sponsored and criminal threat actor groups in China.

The current geopolitical tensions between China and several other nations likely explain the large number of samples of malware in the Chinese language and the month over month increase reflected in our data sets.

MONTH OVER MONTH TRENDS - CHINESE



- In early 2021, Chinese nexus threat actor groups including **RedEcho** were observed targeting the power sector in India.
- In early 2021, multiple Chinese threat actors, including **Microceen, KarmaPanda, Calypso, Stalker Panda, Wicked Panda,** and **Emissary Panda,** were observed leveraging a chain of vulnerabilities in Microsoft Exchange.
- In early 2021, **Stone Panda** (China) targeted Indian vaccine makers SII and Bharat Biotech, exfiltrating intellectual property.
- **APT 41** (China) used a new tool known as Biopass RAT to sniff victims via livestreaming. An attack on Air India in March 2021 was also attributed to the group.
- **ThunderCats** (China) allegedly hacked Russia's FSB using Mail-O malware, a possible variant of PhantomNet or SManager

- **TA413** (China) used the FriarFox browser extension to target Gmail accounts of Tibetan organizations.
- **Judgment Panda** (China) was observed conducting espionage operations against Mongolian, Russian, French, and US targets.
- In May, the group known as **TaskMasters** (China) was observed targeting energy enterprises, government agencies, and transport companies in Russia.
- **Mustang Panda** (China) reportedly targeted an Indonesian intelligence agency in March 2021 and later conducted an espionage campaign dubbed Operation Diànxùn to target telecommunications companies using malware masquerading as Flash applications.
- **Aquatic Panda** (China) was observed leveraging the Log4j (CVE-2021-44228) vulnerability in late December to target an unspecified academic institution.
- In early 2021, **Rocke** (China) was observed using a new cryptojacking malware dubbed Pro-Ocean.
- **Hafnium** (China) was observed leveraging the Log4j vulnerability.
- **Gelsemium** (China) were responsible for a supply-chain attack used for a cyberespionage operation targeting online-gaming communities in Asia.
- Chinese threat actor groups **Calypso** and **Redfoxtrot** reportedly targeted the mail server of Roshan, a telecommunications firm based in Afghanistan.

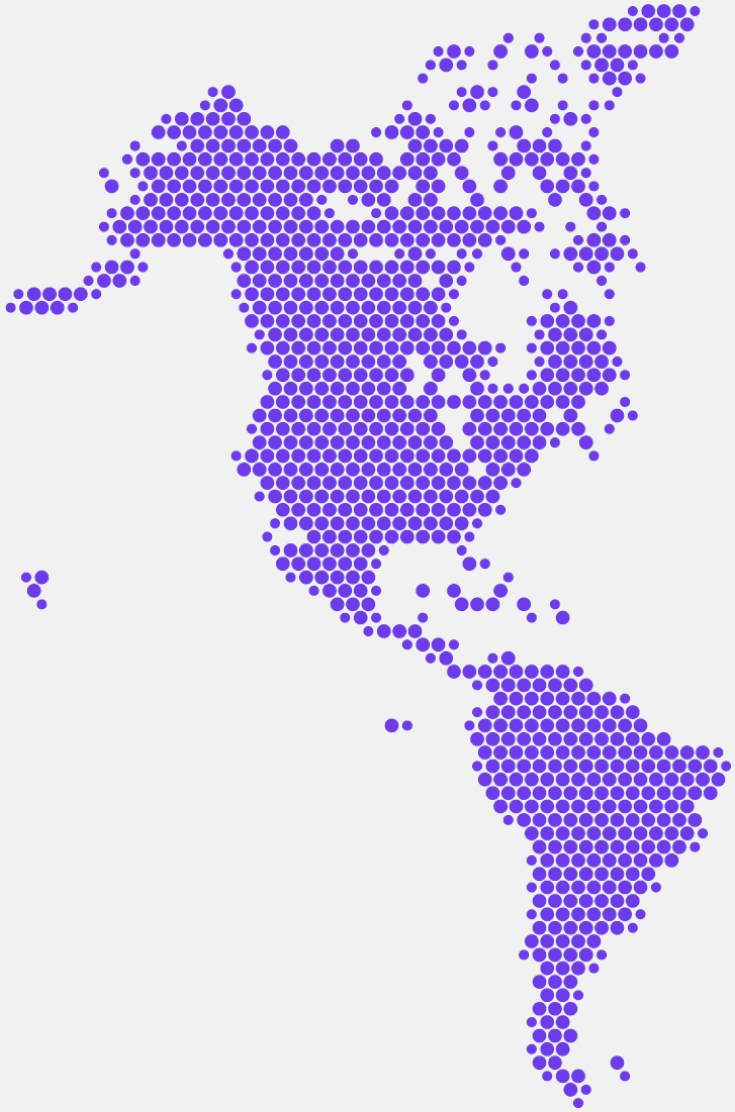
Korean was the second most prevalent language among malware samples. BothNorth Korean and South Korean threat actor groups conducted espionage campaigns.

- In mid-2021, **Kimsuky** (North Korea) reportedly breached the internal network of the South Korean Atomic Energy Research Institute (KAERI) and used malicious blog posts to deliver malware to high-profile South Korean targets.
- In late 2021, **Lazarus Group** (North Korea) was observed targeting security researchers with a trojanized pirated version of IDA Pro. IDA Pro is a reverse engineering software often used by malware researchers.
- **Reaper** (North Korea) ran a surveillance campaign targeting North Korean defectors, journalists, and government organizations in the Korean Peninsula. They used both Windows and Android malware in this campaign. Reaper also began using new TTPs including browser exploits leveraging CVE-2020-1380 and CVE-2021-26411 and the BlueLight malware family. Industry researchers also linked a new version of Konni RAT to a Reaper campaign targeting Russian entities.
- Industry researchers reported threat actor group **DarkHotel** (South Korea) shifted TTPs to use a new attack chain.

Other threat actors in the region also conducted espionage related campaigns.

- Threat actor group **Confucius** (India), who may be affiliated with **Patchwork**, used Pegasus spyware related lures to target the Pakistani military.
- **Mythic Leopard** (Pakistan) conducted a new campaign using malicious MS Office documents to distribute ObliqueRAT to target organizations in South East Asia.

AMERICAS



PolySwarm does not currently track malware by volume for languages used in the AMERICAS region. However, our intelligence analysts track threat actor activity across all regions.

- In 2021, **Blind Eagle** (Columbia) expanded its targeting of South American countries and Spain using phishing emails and publicly available RATs. The group switches between several RATs, including njRAT, Imminent Monitor, a custom variant of ProyectoRAT. Warzone RAT, Async RAT, Lime RAT, Remcos RAT, and BitRAT. The group appears to be primarily motivated by financial gain.
- A financially motivated threat actor group dubbed **FIN13** has been targeting financial institutions in Mexico since as early as 2016. The group is known to use custom passive backdoors and tools to maintain long term persistence in victim environments.
- A threat actor group known as **Elephant Beetle** or Elefante has been attacking financial institutions in Latin America for at least two years. At present, the threat actor's location is unknown but is speculated to be in the same region.

2021 News Highlights

Significant Ransomware Attacks

- In February, **Kia Motors** and parent company **Hyundai** were allegedly targeted by a DoppelPaymer ransomware attack affecting both internal and customer facing systems. PolySwarm noted an increase in DoppelPaymer samples in February and March 2021.
- In February, Polish game company **CD Projekt Red**, best known for its games Cyberpunk 2077 and The Witcher, suffered a ransomware attack in which threat actors stole the source code for several games.
- In March, **Acer** reportedly suffered a REvil ransomware attack in which threat actors demanded a $50 million USD ransom.
- In March, **Royal Dutch Shell** was the victim of a Clop ransomware attack. PolySwarm data reflected a gradual increase in Clop attacks from February to May 2021.
- In May, the DarkSide ransomware gang attacked **Colonial Pipeline,** an American oil pipeline carrying oil primarily from Texas to the Southeastern US. The Pipeline was forced to temporarily cease operations to contain the attack, creating fuel shortages along the East Coast and leading to a declared state of emergency. PolySwarm saw an increase in DarkSide ransomware samples submitted in May.
- In July, IT solutions developer **Kaseya** suffered a ransomware attack affecting multiple MSPs and their customers. An affiliate of the REvil ransomware gang was reportedly responsible for the attack. PolySwarm saw a significant spike in REvil samples submitted during the June to July timeframe.
- In August, **Accenture**, an IT consultancy agency, suffered a ransomware attack perpetrated by the LockBit ransomware gang.
- In November, **MediaMarkt**, Europe's largest consumer electronics retailer, was the victim of a Hive ransomware attack.
- In December, **Ultimate Kronos Group**, a human resources company relied on by organizations worldwide, suffered a ransomware attack that temporarily crippled HR and payroll operations.

Emerging Malware Threats

- ALPHV BlackCat ransomware is likely to become more prevalent, due to its sophistication. BlackCat includes a highly-customizable feature set allowing for attacks on a wide range of targets and can infect both Windows and Linux machines. BlackCat is written in Rust, a language seldom used by ransomware developers. BlackCat ransomware is being promoted on Russian language hacking forums. At present, no known decryptor exists.
- Research by Nokia found a sharp increase in banking malware threats targeting mobile devices, particularly Android devices. The increase is linked to more widespread use of mobile banking apps and is likely to continue well into 2022.

TTPs

- Europol's 2021 Internet Organised Crime Threat Assessment (IOCTA) noted a shift in targeting strategy among ransomware gangs. Some gangs, including the threat actors behind Maze ransomware, are choosing targets based on their financial capability to comply with higher ransom demands and their need to quickly resume operations.
- As the US and other countries continue to crack down on ransomware and encourage victims to refuse to pay ransom, threat actors are becoming more desperate and seeking new tactics to demand a payout. Several threat actor groups recently adopted DDoS as a secondary extortion tactic.

The Fight Against Ransomware

- In April, the US Department of Justice created the Ransomware and Digital Extortion Task Force with the goal of disrupting, investigating, and prosecuting ransomware related activity.
- The US State Department's Transnational Organized Crime Rewards Program (TOCRP) offered a $10 million bounty for information on REvil (Sodinokibi) threat actors and $5 million leading to the arrest of affiliated individuals. The State Department is also offering a $10 million reward for information leading to the identification, arrest, or conviction of DarkSide ransomware gang threat actors.
- In October 2021, 30 countries including the US held a summit to formulate transnational strategies to combat ransomware.
- US Cyber Command recently reported it has taken offensive action to combat threat actor groups who have launched ransomware attacks on US companies.This is one of the first acknowledgments by Cyber Command of taking such actions, targeting criminal threat actors and not just state sponsored espionage groups.

Arrests

- In June 2021, the Ransomware and Digital Extortion Task Force arrested Latvian national Alla Witte due to her involvement in the ransomware gang behind TrickBot. Two other individuals affiliated with TrickBot were arrested outside of Russia around the same time.
- Ukrainian authorities arrested and charged six people allegedly associated with the CLOP ransomware group.
- BlackMatter ransomware group announced they will be ceasing operations, citing pressure from local authorities and an absence of key members.
- Several members of the REvil ransomware gang were arrested in 2021. Yaroslav Vasinskyi, a Ukrainian national who took part in the attack on Kaseya, was arrested in Poland. The US seeks his extradition. The US Department of Justice seized $6.1 million in cryptocurrency payments traced to another REvil affiliate, Russian national Yevgeniy Igorevich Polyanin. This continues the US crackdown on ransomware threat actors. Authorities reportedly arrested at least seven individuals linked to REvil and GandCrab ransomware groups since February 2021.
- Russian national Aleksandr Grichishkin was sentenced to a 60 month prison term for his involvement in running a bulletproof hosting service. His infrastructure was known to host Zeus, SpyEye, Citadel, and the Blackhole Exploit Kit.

Story of the Year: Apache Log4j Vulnerability (CVE-2021-44228)

For 2021, the story of the year emerged in early December. The Apache Log4j Vulnerability (**CVE-2021-44228**), also known as Log4Shell or LogJam, is a vulnerability in versions 2.0 through 2.14.1 of Apache Log4j, a Java based logging tool included in many open source libraries and used in various popular software applications. The vulnerability, which is rated as a 10/10 in severity, is possible due to improper input validation and can be exploited for remote code execution (RCE) attacks to give a threat actor complete access to a victim system.

Multiple malware families were observed exploiting **CVE-2021-44228,** including Muhstik, Mirai, Elknot, Kinsing, M8220, SitesLoader, XMRig, Swrort, Khonsari, Orcus, Tsunami, Monero, WinGo, Nanocore, PowerShell ReverseShell, TellYouThePass, Dofloo, Dridex, Meterpreter, Wiper-rm, and others.

Google reportedly discovered at least 35,863 Java packages using a vulnerable version of Log4j. Companies known to be affected by **CVE-2021-44228** included Apple, Tencent, Twitter, Baidu, Steam, Minecraft, Cloudflare, Amazon, Tesla, Palo Alto Networks, IBM, Pulse Secure, ElasticSearch, Apache, Google, Webex, LinkedIn, Cisco, and VMware.

Critically, Log4j is also used in many external or internet-facing industrial control systems, potentially leaving critical infrastructure exposed to remote exploitation. Sprawling dependencies found in enterprise Java environments, likely leave many organizations unaware they are using a vulnerable Log4j version, particularly when using a third party software product leveraging the library. For this reason, there is a high likelihood Log4j will be overlooked and not patched by some end users. Therefore, it is likely this vulnerability will be exploited for years to come.

At least three additional exploits related to Log4j were discovered, and the original fix to address **CVE-2021-44228** was deemed incomplete in many configurations. The new vulnerabilities, covered under **CVE-2021-45046,** allow attackers to craft malicious input data using a JNDI Lookup pattern, resulting in a denial of service (DOS) attack. Security firm Praetorian warned of a third security vulnerability in Log4j version 2.15.0 that was released to fix the initial vulnerability. Threat actors can potentially use this third vulnerability to exfiltrate sensitive data. Trend Micro later released information on yet another vulnerability, **CVE-2021-45105,** leading to denial of service via uncontrolled recursion in Log4j StrSubstitutor. They stated it is not a variant of **CVE-2021-44228** but abuses a similar attack vector. An additional vulnerability, **CVE-2021-44832,** was discovered in late December. **CVE-2021-44832** affects Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4), making them vulnerable to an RCE attack when the configuration uses a JDBC Appender with a JNDI LDAP data source URI, when an attacker has control of the target LDAP server.

A major bug was discovered in Log4j versions 2.8 - 2.16. If a string substitution is attempted for any reason on the following string, it will trigger an infinite recursion, and the application will crash: ${${::-${::-$${::-j}}}}.
Some threat actors began using novel TTPs when exploiting **CVE-2021-44228.** Instead of using LDAP callback URLs, some threat actors used RMI or both LDAP and RMI in a single request to maximize chances of success. So far, the threat actors observed using this technique were attempting to hijack resources to mine Monero, a liquid cryptocurrency with extensive anonymity features. However, other threat actors could adopt this method. Another security research firm reportedly discovered an alternative attack vector affecting services running as localhost that are not exposed to any network or the internet. It relies on a basic Javascript WebSocket connection to trigger RCE on servers locally, via drive-by compromise. In other words, anyone with a vulnerable Log4j version can be exploited via the path of a listening server on their machine, or local network through visiting a website, and triggering the vulnerability.

A worm leveraging **CVE-2021-44228,** a self-propagating Mirai bot targeting Linux systems, emerged but proved to be ineffective for large scale attacks.

Industry reporting indicates state sponsored APT groups, including Hafnium, Stone Panda (APT 10), Aquatic Panda, Nemesis Kitten, Charming Kitten (APT 35), Venomous Bear (Turla), Fancy Bear (APT28. and unnamed North Korean and Turkish threat actors may be leveraging **CVE-2021-44228.** Financially motivated groups of Eastern European nexus, including the Conti ransomware group, are also reportedly leveraging **CVE-2021-44228.**

Appendix A: Growing List of PolySwarm Ransomware Families Tracked

Alphastealer
Anchor
Antefrigus
Avaddon
Bazaar
BazaLoader
Betasup
Biglock
BitPaymer
Blackclaw
Blackout
Buran
Cerber
Clop
Conti
Creepy
Crypt32
Cryptomix
CrySIS
Darkside
Deathransom
Defray
Demonware
Dharma
Dogecrypt
DopplePaymer
Duduer
Dusk
Egregor
Ekans
Exorcist
Fuckunicorn
Gandcrab
Garrantydecrypt
Gomer
Gracewire
Hackransom
Hakbit
Infodot
Jackpot
JSworm
Lanifynop
Lockbit
Makop
MassLogger
Maze
Medusalocker
MegaCortex
Mountlocker
Nemty
Netwalker
Ordinypt
Ouroboros
Paradise
Phobos
PonyFinal
Prolock
Qulab
Raccoon
RagnarLocker
Ragnarok
RansomExx
Revil/Sodinokibi
Robbinhood
Ryuk
Samsamjaythl
Satancryptor
Scarab_monster
Sekhmet
Smaug
Teslacrypt
Tongda
Troldesh
Ursnif
Vatet
Wannacry
WastedLocker
Whadrama
Macaw
AstroLocker
BlackMatter
Hive
BlackByte
Prometey

Appendix B: Sample IOCs

This page includes a limited selection of hashes for some of the samples we have available for malware listed in this report. Contact us for more information.

Hexane
6de242a47cadf445a3a1f7d4a99109665351bbcb55a56993ad6bb61c6abff80a
1990855b7891bad65dae35d98d9b05eb1ba73dcf699ffd4d68a0b91afb6c024b
a50bd3044c03a07ec626460660e6428fde6d8a708d8a7ae7c261b1f6fd2dfe8f
860158c654251bdcb200b0a73e43b82bddd4813b603481472c9845ee7fcf0959
f00e690f57314be6e58e5fe6825d999d59f830dd7a7f38c651c9501d11ad3a3c

Static Kitten
0a1a95822404644c13db06c7d3f45a69f0718d518079408df11efa5dbff8ee16
45f28609c90c89acf03ce88c29043b9983e274e54e7486a3cf40e6bcf0dc2ad4
1557d654347da9e525f17573a8c686f3593f82d30a2ee05270428af96a06fa3c
f0f5157eed688ef19bd5f5bf001b3bd116dd42589081fd8f4f06af242e3f3c4c
e0da3216c68e94fa5dde9c58b06eb56decc80a65f6a235a99e54b73fcd586c67

Charming Kitten
942dcfb1c82c97f3f31d562a02d6a7d31f25432da6759be28617ca0b05b25053
4e0c4889cf60777ddd37efd00172491c99159a0c0eb2a4adab953deb3f26f02d
719b08101de5736dc7e0a26cc29412618657ba6a6f3a5443e5f88a361f322be0
7df9e34304f2b6d97e0628dc492e5ff0af99299d62619acbaa163aaedbbd18fb
f2b8e5dd6e1677398c78e9e1c207ba4a7c727798fa68ae958b586fa00e1c114a

OilRig
c98716342b9cf98625f5ebcd05d1139e3fcd5a5b0e2887931573974e30163280
2bd86a68691266180f48b3adf808bc214a6c2a478b500c2f05df7dc362c5f273
8707537f3e3754c7574422942929e67afe8cae13541fea49bf36e5a6573d6f3f
1b773569b4c34472f9159bf7cc3438b21c3c32f4d2c170449920c85cd4a2f29c
f7bb0fb0dc0e2ba90a0eb8d3d41b1a311c58835558f74d7c3bc7393adbb275d5

Strong Pity
b46b0c11c1e1f103ea32491d61526896f86939f7a7ce39f020f0097d729f4c11
7ffcae7a794b77f088fb56e233ffc63c7f8fdc3e6e016e98f73d0d78e2344225
ec696c8ade72dc73987e85f90beeb9f1eb7283eb8516267390820a01c7121e77
fe59e9d6f663513d5533af0b04bfd1df140bc52c4abda9710c81f26aed7c98d7
fcf2edee6aab6e72597903a284a654b7916655d808d536ef6bdced0c6df48a76