Trellix ADVANCED RESEARCH CENTER

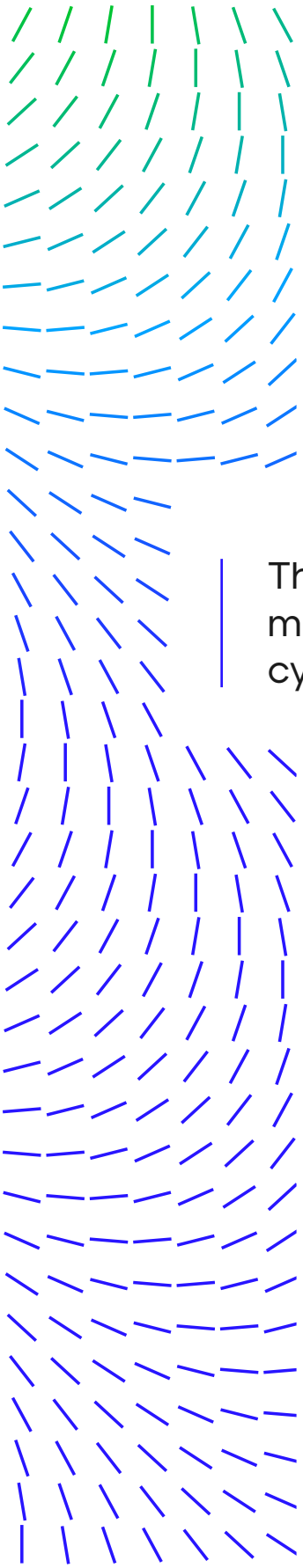
2023 Threat Predictions

Every year, we look into our crystal balls and share our thoughts on what the next year in cyberthreats may look like. The Advanced Research Center team's work has informed predictions spanning from hacktivism to cyberwar to the software supply chain.

We started 2022 with an industry-wide vulnerability in Log4J, which was closely followed by cyber and physical war targeting Ukraine. We're closing the year observing hacktivists taking matters into their own hands, new actors in operation, and a changed but increasingly active ransomware landscape. As stress continues to weigh on the global economy, organizations should expect increased activity from threat actors looking to advance their own agenda – whether for political or financial gain.

To outwit and outpace bad actors and advance defenses proactively, security must be always-on and always learning. Our team studies new cyber activity, develops threat indicators to make our security products smarter, and publishes research that keeps our customers and the industry at large prepared.

Following, researchers across the Trellix Advanced Research Center outline just what the cybersecurity landscape may look like as we move through 2023.



Geopolitics and grey-zone conflict

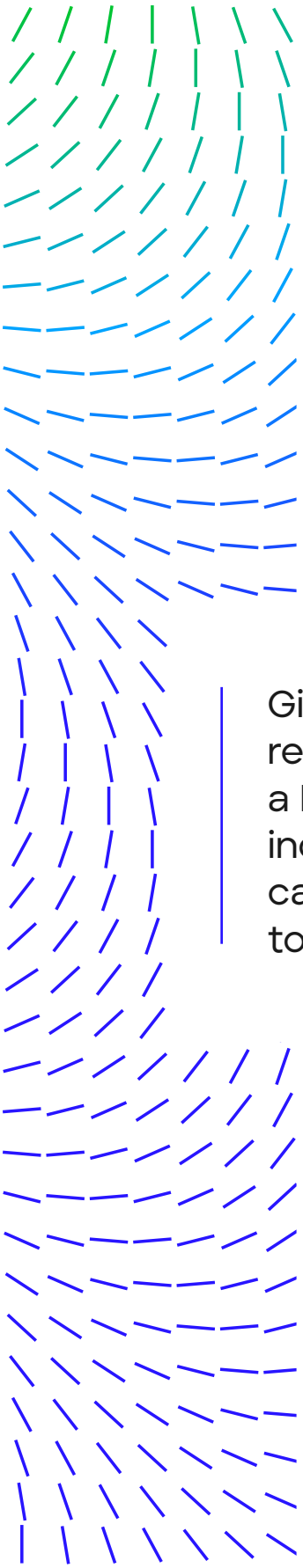
By Anne An

Geopolitics open new avenues for cyberthreat actors to attack businesses and individuals in their targeted countries and supporters. Throughout 2022, geopolitical tensions have been exacerbated by hacktivists and other cyberthreat actors. Cyberattacks have accompanied and complemented kinetic military action in these instances to undermine resistance and defense capabilities against invaders, influence foreign policies, and support the aggressor's strategic goals. Russia's invasion of Ukraine, political tensions in the Taiwan Strait, and North Korea's missile tests over Japan and South Korea have all been aggravated by accompanying cyberthreat activities.

> The rise of geopolitically motivated cyberattacks and misinformation campaigns may continue to shape the cyberthreat landscape through 2023.

The Russian invasion of Ukraine in February 2022 triggered a new wave of destructive cyberattacks and misinformation campaigns against the Ukrainian government, military, and commercial organizations. Countries supporting Ukraine such as the United States and NATO countries have also been targeted. These cyber-enabled threats are part of Russia's concerted measures to harm and destabilize targets while maintaining deniability. If the war continues into 2023, Russian threat actors may likely continue targeting Ukraine's public, energy, financial, business, and non-profit sectors while using propaganda and disinformation campaigns to wage war.

In the case of Taiwan, Trellix telemetry data suggests threat activities targeting the Taiwan government and commercial organizations likely began when Pelosi confirmed her trip to Asia, even several days before the publicly reported DDoS attacks against Taiwan's presidential office and other government agencies. These efforts could have been intended to influence Pelosi's decision to visit Taiwan. These successful cyberattacks carried out by hacktivists and other cyber threat actors may likely lead to more cyberattacks to support military action or instill fears in future China-Taiwan crises. Similar tactics could later be leveraged against Taiwan's regional partners such as Japan and South Korea and supporters such as the United States. China may also likely continue to engage in disinformation or propaganda through funding and channeling pro-Beijing media platforms in Taiwan to erode Taiwan's democratic institutions.



Another example was spikes in detections of malicious activities from North Korea's Lazarus Group closely corresponding to the periods when the DPRK government launched ballistic missiles over Japan and South Korea in September and October 2022. These attempts were likely part of increasing active or passive reconnaissance efforts to support the process of launching ballistic missiles. We may see similar threat patterns against South Korea, its regional partners, and its ally the U.S. through 2023 as North Korea's offensive cyber operations continue to serve the government agenda, specifically its nuclear and ballistic missile programs.

Hacktivism moves to the center stage

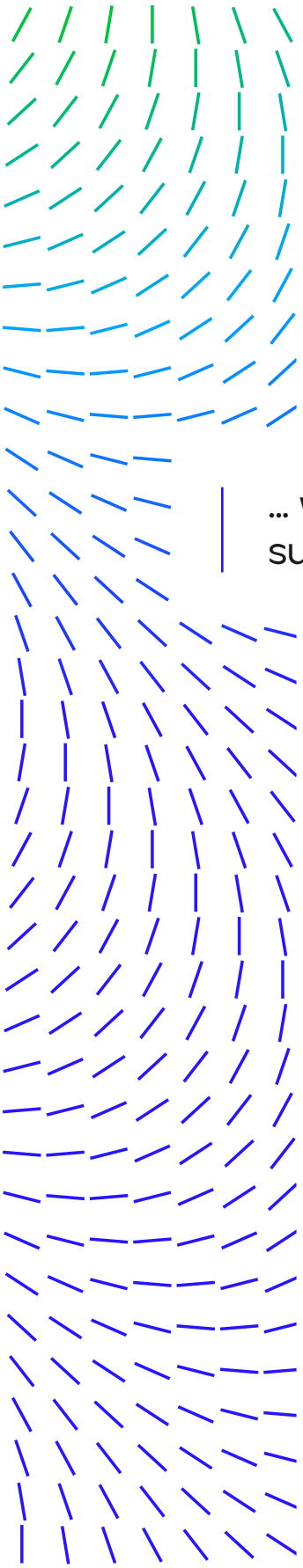
By Manoj Reddy

For many years the global headlines have been dominated by state-sponsored and financially motivated cyberthreats. Hacktivism - politically or socially motivated hacking by activists - has remained in the background in recent years.

Given current global tensions, we are already seeing re-emergence of hacktivism and expect this to play a larger part in 2023. As groups of loosely organized individuals fueled by propaganda align for a common cause, they may continue to ramp up their use of cyber tools to voice their anger and cause disruption.

Patriotic hacktivism increased in 2022 as war and other conflicts continue, and it breaks down into broad streams of actions like DDoS attacks, defacements, doxxing, intrusions, and leaking of personally identifiable information (PII). Hacktivists are targeting a wide range of industries and sectors that don't align with their ideological and political views, including telecommunication, energy, aviation, technology, media, and government sectors. There are many examples of this activity in recent history related to the Russian and Ukrainian war including the attacks against websites in countries publicly supporting Ukraine by Russian hacktivist group Killnet and another Russian group targeting Ukraine's largest private energy company.

As tensions in 2023 are expected to rise, we expect hacktivism to continue to scale as it suits the political agenda of opposing parties and offers perfect plausible deniability for actions since they are initiated and undertaken by activists.



Skeletons in the software closet will multiply

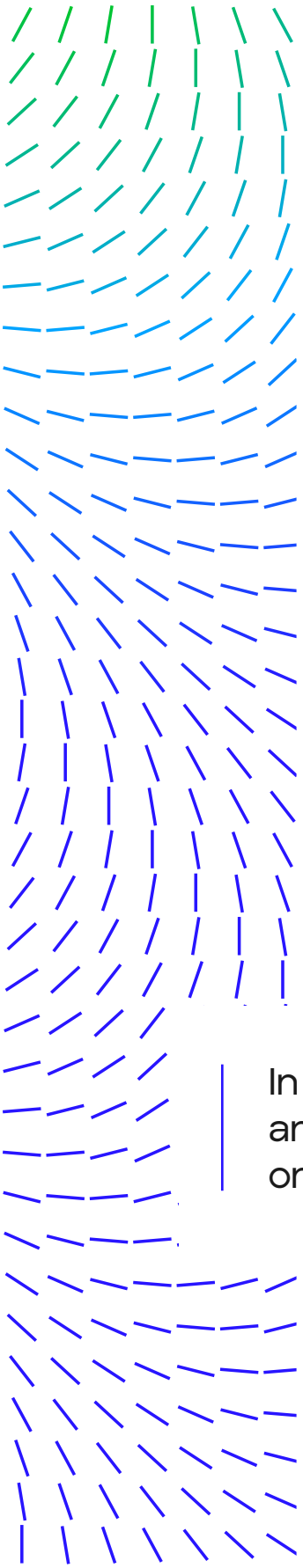
By Doug McKee

In 2022 we saw a continued rise and attention brought to supply chain attacks and attack vectors. IBM included them in their annual breach report highlighting an impressive 19% of all breaches are a result of supply chain issues. While we continue to concretely define exactly everything that is classified under this umbrella, vulnerabilities in critical underlying frameworks are undisputedly part of the supply chain. If we consider what Log4J did in late 2021 as just the beginning of the appeal this attack surface presents to threat actors,

> … we expect to see an increase in breaches related to supply chain issues in 2023.

It's without surprise: hackers are lazy. They wish to incur the largest amount of financial gain or – especially in the case of nation states – inflict the most amount of damage with the least amount of effort. As much as big players like Microsoft and Apple get slammed with negative press for the number of vulnerabilities discovered in their products, the truth is, over the last several decades it has been increasingly harder to find and successfully exploit vulnerabilities on these platforms. This is one of many reasons why exploiting the human factor is still so crucial and executed by threat groups. However, this increase in difficulty also sends hackers looking for easier targets in other areas. Not all popular frameworks, libraries, and SDKs which have been around for a long time have kept pace with regular security audits and modifications required to ensure their security resilience, especially in the open-source community.

Both threat actors and security researchers are likely to heighten their study of the underlying frameworks which are part of the supply chain. As a result, we anticipate seeing more vulnerabilities discovered (or rediscovered) and exploited which have a wide impact, that won't necessarily come in the form of a major Microsoft bug, but a framework you may have never heard of that everyone is using. Therefore, we must increase our visibility and in-depth understanding of exactly what code we have running within our organization.



Increasing activity by teen cybercriminals at every scale

By Rhonda Leopold

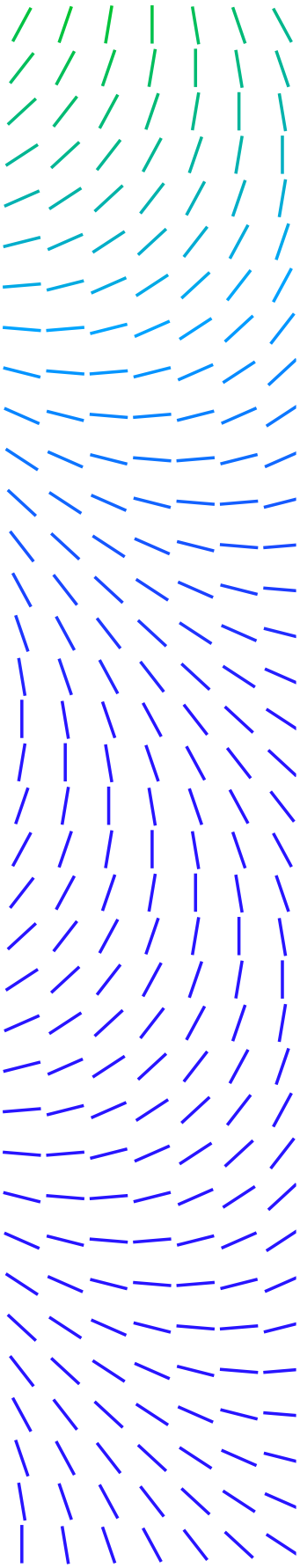
Online scams cost our economy billions of dollars each year. The security budgets of schools, hospitals, and corporations will continue to increase, yet teaching our children not to be a scammer or steal online is not yet baked into society. Where petty theft and harassment online are concerned, there is still some work to be done to communicate the dangers of children becoming cyber criminals. Keeping one's kids safe online is the primary focus of parents; however, they should also be concerned that their child is being ethical online. Illegal downloads of movies, college textbooks, software, and games are often viewed by kids as more of a challenge than a crime. At times, parents even encourage this behavior which is why education needs to happen at all levels.

We are seeing technically talented young people being recruited by bad actors and organizations. Beginning in late 2021 a 16-year-old allegedly led successful hacks of international organizations like Microsoft, NVIDIA, Okta and Samsung under the guise of the Lapsus$ gang. These cybercriminal organizations are today the talent competition of Fortune 500 companies and security companies who all work to protect society online.

There are some global initiatives to help prevent our youngsters from sliding off into a world of cyber-crime. To educate the young on the dangers of cybercrime, there are some new initiatives like Hackshield that teaches kids about the dangers through gaming. But the generational gap needs to be addressed and parents need to be educated to ensure they are leading their children away from petty cybercrime or even more nefarious crimes.

> In 2023, we expect to see increased activity from teens and young adults – everything from large-scale attacks on enterprises and governments to low level crime …

targeting family, friends, peers, and strangers to make a quick buck, cause embarrassment, test new skills and gain social capital. This problem may grow, budget increases will follow, and costs will continue to be handed back down to us as consumers. Teaching children what a crime is at the keyboard is essential.



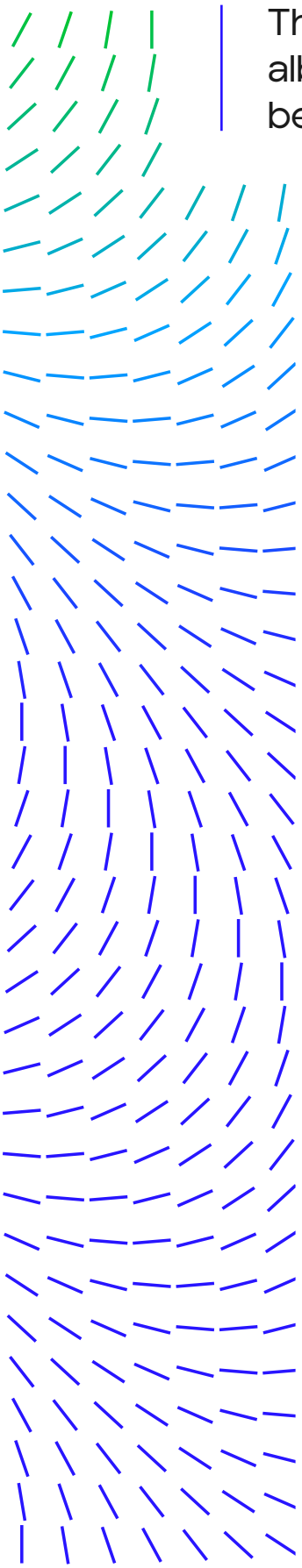
Declining accuracy of code-based attribution

By Max Kersten

In today's world, digital threats are overwhelming. The internet offers unprecedented anonymity to many, but every so often a mistake is made. These mistakes, or breadcrumbs if you will, allow investigators and researchers to track actors. With regards to cybersecurity, attribution is often heavily based upon dissected malware samples. It has been proven time and again that coding styles can be linked to actors, much like someone's handwriting. Over time, malware development diversified: actors aren't purely opportunistic criminals who seek illegal financial gain, but rather highly organized and specialized professionals, still seeking illegal financial gain. Such a claim isn't meant as a true-or-false statement, but rather to show how numerous groups have developed over time, while others remain opportunistic.

Attribution purely based on code alone can, however, pose a problem. Whereas advanced espionage groups are often known to create their own tooling for their campaigns to preserve their secrecy, some other malware types do not require such secrecy per se. Prime examples of such malware are wipers. Once a wiper is used, it isn't novel anymore, and the detection and prevention of the malware is bound to be implemented. The creation of malware is often thought to be done by coders, who then sell the malware-as-a-service, or work with affiliates. Creation can also be outsourced to legitimate contractors, thus obscuring the code base attribution immensely, as the contracted authors have different coding styles. The usage of multiple wipers, with no meaningful code overlap between them, was found in our telemetry in June 2022. At that time, the actor failed to launch the WhisperGate wiper, and tried to resort to HermeticWiper instead, all within three hours' time.

The WhisperGate wiper's code is not linked to HermeticWiper's code, and the assumption that both are used (and potentially made) by the same actor is an unsubstantiated claim based on the samples' code bases alone. While other intelligence might (dis)prove such a claim, it is important to note that the additional context is required for the attribution to make sense. This shows how completely relying on code-based attribution is tricky, especially since not all analysts have access to the required additional context, in contrast to the often widely accessible malicious files themselves.



> The decrease of accuracy of code-based attribution, albeit seemingly insignificant on its own, is likely to become more problematic in the future, ...

especially when taking the re-use of (leaked) malware source code and the collaboration between actors in the segmented underground into account. We therefore urge analysts to include their confidence level when making claims that aren't (fully) supported by facts. This provides a clear indication to the reader with regards to the way the report should be perceived, allowing the appropriate actions to be taken from the get-go.

Imminent global cyberthreat to critical infrastructure as cyberwarfare evolves

By John Borrero Rodriguez

Since the Russian invasion of Ukraine, cyberattacks have evolved drastically not just from nation states, but also from cybercriminals, hacktivists, and other less skilled actors. Tactics targeting critical infrastructure have plagued the cyberwar landscape. The current patterns of tactics currently observed suggest increased aggression and risk to a plethora of entities. Similarly, a rise in victims of cyberwarfare collateral damage has been observed. These risks may be ever more present to those in critical parts of the energy, banking, and military sectors.

Threat actors such as Turla, Metador and UNC3886 find themselves in the spotlight due to their increased activities. Couple this with some of their novel techniques such as UNC3886's VMware ESXi malicious VIB file persistence and the rise in volatile global conflicts has created a prime opportunity for advance persistent threats (APT) to better adapt, expand, and conduct their campaigns.

In 2023, no longer will simple security planning be enough to deter or prevent attackers. System defenders worldwide may have to implement a more proactive defensive approach led by the stringent industry standards followed by government, military, and multi-governance environments. It may very well be a significant rise in advanced cyberactors causing disruptions to critical infrastructure in vulnerable targets. No doubt the discovery of novel techniques may cause other bad actors to adopt them, changing their campaigns to further threaten users, industries, and critical assets connected to the internet.

Cyberwarfare remains an ever-changing landscape, with sympathetic users being called to act against adversary targets and unsuspecting users being used through fictitious applications and campaigns. We suspect we could see a rise in unsuspecting users being leveraged as launching points for attacks targeting critical infrastructure.

Further increasing the threat to critical infrastructure, we could see more IoT devices hijacked in exponentially larger distributed denial of service attacks for warfare purposes.

With more collaboration comes more phishing

By Jaspreet Singh

In 2023 we expect to see weaponized phishing attacks spread their wings across commonly used business communication services and apps.

Smishing, vishing, social media phishing and business email compromise attacks have traditionally been managed with anti-phishing toolbars and email security protections, but in near future phishing may scale beyond email and messages, spreading across communication channels in a much stealthier way.

Messaging channels and business collaboration apps like Slack, Teams, ClickUp, ProofHub, Chanty and others are critical for organizations to ease their communications and simplify collaboration. The added layer of AI-driven development of more sophisticated phishing emails with advanced methods further complicates the landscape for phishing. While Zoombombing and similar methods have been observed, we expect the use of business collaboration apps to grow as a threat vector.

Threat actors globally may boost and tweak their established methods to infiltrate and excavate into organizations network. While hybrid work culture has expanded the attack surfaces to individual's vulnerable and poorly managed home networks and devices, threat actors have benefitted by using this as a medium to easily target the corporate networks. This has driven increases in phishing attempts targeting companies, and in turn organizations have focused on strengthening their perimeters and email protection services. Keeping eye on new tactics and

techniques targeted towards other communication channels should not be overlooked and neglected in the new year.

"Alexa, start mining bitcoins"

By Ajeeth Srinivasan

With the world around us moving more into the digital age, IoT devices are a part of our daily lives. We have smart devices that can drive our vehicles, keep our coffee warm and open doors for us. Interestingly there is a flip side to this when these devices or functionalities start going rogue.

Coinminers have always been known for their quiet nature of remaining in the shadows and using system resources to mine for cryptocurrencies. With the recent trend of devices becoming more proficient and advanced, the capable hardware of these devices could be leveraged by hackers to mine cryptocurrencies at your electrical expense. The worst part is these devices can be used by nation-state or APT groups to spy on high profile targets just like we saw with Pegasus. With no proper anti malware solutions available for these smart devices, security analysts may struggle to reverse engineer malware manually.

Cryptomining demands huge resources and with the recent variations in cryptocurrency values, mining cryptocurrency legitimately will not be the best option. While a single IoT device may not contribute hugely to crytomining, a botnet like Mirai can bring thousands of devices under a single umbrella. There have been cases of Coinminers jumping from IoT devices to other operating system's and since security is not at the forefront while manufacturing IoT devices,

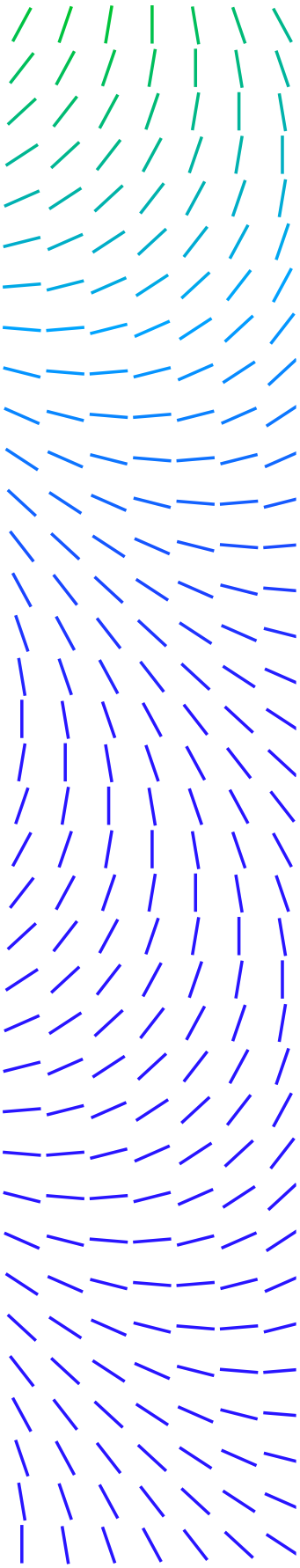
... we predict cryptomining via IoT devices to ramp up.

Space hacking: only going up from here!

By Ryan Fisher

With the launch of more satellites, society's reliance on satellite data and internet access,

... the attack surface will grow, and history has shown us that attacks usually follow. We expect the compromise of satellites and other space assets may increase and become more public in 2023.

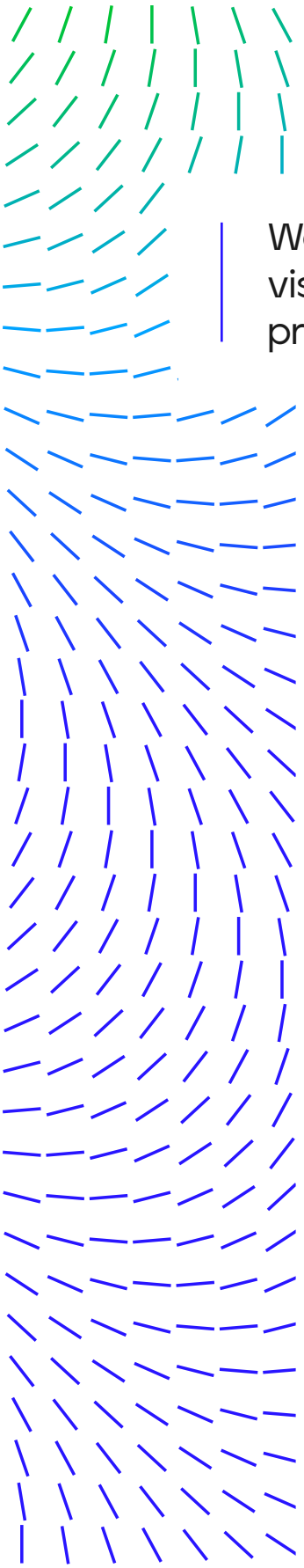


Between the launch of the first satellite, Sputnik, in 1957 and 2019, less than 600 satellites were launched per year. However, that number rocketed to over 1800 satellites in 2021 and 2022 will see even more. We see risks to satellites highlighted in the fact that satellites are purpose-built computers and as such, are vulnerable to many of the same cybersecurity threats that happen here on earth. Compromising the ground control for a satellite was first demonstrated in 1998 when hackers compromised the computer network of NASA by hacking into the Goddard Space Flight Center in Maryland. They then instructed ROSAT (an X-Ray satellite) to aim its solar panels directly at the sun. This fried the batteries and rendered the satellite useless. However, breaching a ground control station isn't always necessary especially with the proliferation of smaller and cheaper "CubeSats" that use off the shelf parts to keep costs low. This, combined with relatively inexpensive ground-based communication equipment means that hacking some of these CubeSats may be as simple as waiting for one of them to pass overhead and then sending malicious commands to exploit vulnerabilities in the commodity hardware or software of the satellite.

As the cost to put payloads into low earth orbit (LEO) continues to decrease, more and more companies will have satellites launched. And as is the case in other industries if cybersecurity is not fully considered during initial phases of design it will take a back seat to other engineering challenges thus leaving the system open to compromise.

Targeted denial-of-service attacks like those witnessed in Ukraine against SpaceX Starlink terminals may be an ever-increasing problem. In Starlink's case they were immediately able to shift resources to cybersecurity to address the jamming, however not all satellite companies will be as agile. An example of this is seen with the KA-SAT SATCOM attack that Viasat experienced which coincided with the physical attack Russia initiated against Ukraine on February 24, 2022. Tens of thousands of SATCOM terminals suddenly stopped working in several European countries including Ukraine. Full details have not been released but the current theory is that a misconfiguration in the management network allowed attackers to compromise/spoof a ground station and issue commands which deployed a malicious firmware update to the terminals knocking them offline.

Another area of concern is ransomware. As the space landscape continues to evolve from purely scientific research into critical infrastructure it brings with it malicious actors which prey on critical infrastructure knowing the value of the services provided by these networks. Locking up critical infrastructure satellites and demanding a ransom from the providers or even the businesses using the links will result in lucrative payouts for ransomware authors as these networks cannot remain offline for long.



Here's my number, so call me, maybe?

By Daksh Kapur

We anticipate a significant increase in reverse-vishing attacks, with less tech-aware users being the prime target.

Reverse vishing is a redolent of vishing (voice phishing) where the potential victims are being cold called by attackers, except in the case targeted users must dial the number. The phone number might be provided to the victims as part of an email, SMS etc. involving an urgent notification like bank transaction or order cancellation which compels the victim into calling the mentioned number.

Up until recently, attackers have been majorly utilizing traditional email attack vectors like attachments and URLs to deliver malware or harvest credentials. In such attacks, security products focus on scanning the attachment/URL and provide detection based on the scan verdict.

The tricky part with reverse-vishing campaigns is that it does not contain any malicious traditional entity like a URL or attachment which has been used in email-based attacks, but rather contains a phone number which the user must call and from there onwards, the attacker holds the stage now and its upon his act to convince the caller into installing a malware or conduct financial/credential fraud. This creates a challenge for security companies as the scanning techniques based on traditional attack vectors would not be suitable in such cases.

It is possible to somewhat control such attacks by authoring detection rules based on the pattern of the email content combined with other email parameters like screenshot, addresses, and IPs. The detection rules and parameters need to be constantly updated to match the pace of evolution of tactics utilized by adversaries. Our constant research on such attacks allows us to provide progressive detection from such attacks.

We have seen that reverse-vishing cases have increased by more than 500 percent since 2021 and it doesn't seem to be going down.

It gets more troubling as adversaries have spread their claws to hit victims from different mediums like text and third-party messaging apps like WhatsApp and information mediums like Google Reviews. This is even more of an issue as it is tricky to regulate such content in the above-mentioned mediums, so it becomes a tunnel for attacks to slip by.

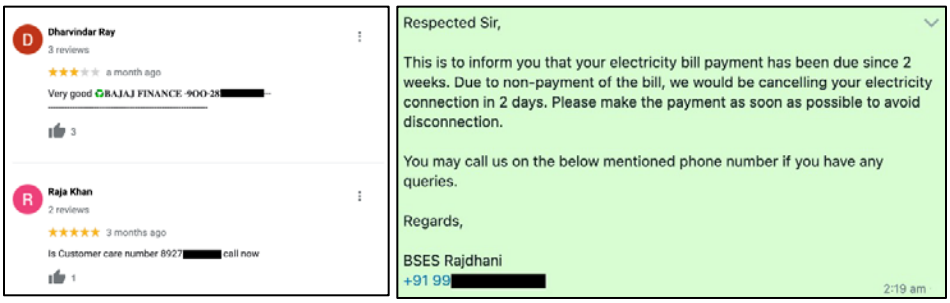


Figure 1 - Examples of reverse-vishing attacks delivered through non-email-based mediums

More research is required to detect such attacks in an efficient way and until that happens, reverse-vishing is going to be abounding and the people who are less tech-aware may be most affected.

Attacks against Windows domain will scale

By Bing Sun

Taking over the entire Windows Domain/Active Directory – or an organization's entire network – is the ultimate goal of many targeted attacks against a Windows ecosystem. Once the attacker gets the initial footholds into an organization's internal network, the next thing to do is to move to other critical systems, such as a Windows Domain Controller, and to further compromise the entire domain. To achieve this goal, the attacker must leverage certain vulnerabilities to escalate the user privileges, for example, CVE-2021-42287/CVE-2021-42278 (Active Directory Domain Services Elevation of Privilege Vulnerability, aka noPac) can be exploited to grant the attacker a service ticket representing the domain administrator.

In a typical attack scenario, the attacker usually enters the internal network as a basic user (low privileged), however as an authenticated user (meaning already being a member of the domain) they can exploit a domain privilege escalation vulnerability to escalate himself/herself to the domain administrator. After that, the attacker can use the classic domain attack techniques, such as Golden Tickets, Silver Tickets or DCSync to retrieve sensitive information and maintain persistent access to the critical domain resources.

Windows Doman/Active Directory is a critical and complex system that involves multiple services and protocols, and any vulnerability in these services or protocols could be exploited to compromise the whole system, which then gives the attacker full access to organization's sensitive information and enable profit from leaked data. Because of the importance and complexity of Windows Doman/Active Directory system, this "gold

mine" area has drawn a lot of attention from both hackers and security researchers and drives them to work hard on it to find bugs and develop new attack techniques. According to our observation, Microsoft has fixed quite a few Windows Doman/Active Directory and NTLM/Kerberos related vulnerabilities in the past years, and the total number of such vulnerabilities patched each year seems to be on the rise (8 in 2020, 10 in 2021 and 22 in 2022). Moreover, some new exploitation vectors have been discovered, such as NTLM relaying to ADCS and Kerberos relaying attack.

We believe in the coming year more domain privilege escalation vulnerabilities may be discovered and, at the same time, we might continue to see more real-world attacks against Windows with the explicit goal of complete network takeover.

About the Trellix Advanced Research Center

The Trellix Advanced Research Center brings together an elite team of security professionals and researchers to produce insightful and actionable real-time intelligence to propel customer outcomes and the industry at large. Driven by the industry's most comprehensive charter, our skilled researchers detect trends ahead of the market to empower our customers and partners to solve for emerging threats. More at https://www.trellix.com/en-us/advanced-research-center.html.

https://twitter.com/TrellixARC

https://twitter.com/TrellixARCThe information views and opinions expressed herein are the result of research and experience, are provided for educational purposes only, and are not necessarily those of Musarubra US LLC.

072022-05