F-SECURE THREAT HIGHLIGHTS REPORT

February 2022

F-Secure

EXECUTIVE SUMMARY

CONTENTS

FOREWORD

It is the end of February, and it has been a month packed full of global developments and high profile events. The Russia-Ukraine conflict has dominated the news cycles and it is there we start this month's highlights, exploring the cyber elements of the conflict and the wider impacts organizations should be aware of. We expect this situation to continue to develop in the coming weeks and on to keep an eye on incase of further escalation or developments.

Looking elsewhere we have seen a few high profile state-backed threats reported on this month with the use of Cyclops Blink by a Russian based threat actor to exploit devices and an advanced kernel based malware revealed to be in use by a Chinese threat actor.

As always we continue to see developments in the cyber-criminal space, with special focus on data related extortion intrusions this month from Karakurt and LAPSU$ groups. In addition, the CONTI ransomware group suffered a leak of their internal chat systems that has uncovered a wealth of data that could be used by organizations and law enforcement to counter the threat posed by this group.

As always, we hope you enjoy this month's report, and we welcome any feedback you may have.

- Callum Roxan, Head of Threat Intelligence

MONTHLY HIGHLIGHTS

RUSSIA-UKRAINE CONFLICT: RELATED CYBER ACTIVITY

SUMMARY OF MAIN ACTIVITY

On the 23rd of February 2022 Russia began a military invasion of Ukraine. In what has been described as a co-ordinated operation, destructive wiper malware was deployed across critical national infrastructure within Ukraine.

The wiper malware, was deployed at approximately 2022-02-23 15:00~ UTC across targets across Ukraine and at least one other country, Lithuania. The wiper malware has been coined as "HermeticWiper" by SentinelOne based on the use of a code signing certificate from "Hermetica Digital Ltd". Industry analysis suggests the malware is an MBR wiper and it leverages the legitimate EaseUS Partition Manager drivers to conduct its destructive actions.

F-Secure can confirm from our own telemetry that a version of HermeticWiper was deployed against a CNI organization within Ukraine just prior to 2022-02-23 15:00 UTC. The data available to F-Secure suggests this was deployed via group policy, which aligns with observations by other industry partners in their aperture.

Symantec's analysis suggests that the intrusions related to the deployment of the wiper they observed may date back as far as November 2021. In one instance Symantec have claimed the actor exploited a tomcat vulnerability and in another they used malicious SMB traffic against an Exchange server to gain access to victim organizations. The report describes the use of CMD, PowerShell, Certutil, Schtasks and a Webshell in the intrusions.

Symantec also report the deployment of a ransomware strain on victims at the same time as the wiper. The ransomware, named "HermeticRansom" by ESET, is reported to have been deployed via the same mechanisms and at the same time as the wiper malware on some, but not all, victims. Analysis of this ransomware revealed it was written in Go and that it had some errors in the code that means any data encrypted by the ransomware can be decrypted. Avast have released a decryptor for the ransomware.

ESET also managed to identify a worm they have named as "HermeticWizard", which will attempt to spread the HermeticWiper malware across the local network using WMI and SMB. It should be noted that the SMB functionality seems immature and unlikely to be successful.

In addition, ESET also identified another wiper that they have named IsaacWiper, which was deployed against other victims in Ukraine the day after HermeticWiper was observed in use. ESET did not identify any technical overlap between IsaacWiper and HermeticWiper, but timing and victimology suggests some co-ordination between the deployment of these wipers.

WIDER ACTIVITY

The Ukrainian government called on Hacktivists to assist their defence via performing cyber operations against a list of Russian organizations. The Ukraine government setup a telegram channel to co-ordinate these activities. Several hacktivist groups have rallied behind this call and a combination of DDoS, Data Theft and Destructive attacks have reportedly been performed against Russian organizations. In addition, another hacktivist group have conducted attacks against Belarusian organizations to attempt to disrupt their support for the war. Curated Intel have an excellent summary of all the activity on their Github page.

The hacktivist collective Anonymous have released a video and twitter posts in support of Ukraine and have stated they are *"...officially in cyber war against the Russian government"*. Initial actions by the group appear to be focused on disruptive attacks such as distributed denial of service (DDoS) on Russian websites and media.

Ghostsec, an offshoot of Anonymous are also engaging in disruptive attacks against Russian websites and are reporting their intentions and targets on their Telegram group chat.

The ransomware group CONTI released statements on their dark web site, announcing *"full support of Russian government"* and threatening to attack critical infrastructure of the nation's enemies. But have since found themselves in turmoil, as a CONTI affiliate has leaked internal CONTI data including internal communications between members, apparently in support of Ukraine and in defiance of CONTI's earlier statement. The leaks have spread to also include the doxing of members of CONTI and TrickBot.

LockBit, a prolific ransomware group have also released a statement on their dark web site announcing neutrality, stating that their community *"consists of many nationalities of the world"* and that they would not engage in political attacks and were only interested in money.

F-SECURE'S INSIGHT

The Russia-Ukraine conflict has included the apparent combination of destructive cyber capabilities along with more conventional military forces. However, contrary to much prior analysis, these have not appeared to have been as widespread or damaging as predicted.

The use of wiper malware is notable, but its use to date has not suggested we can expect to see widespread use of this against a broader scope of targets. Whilst tensions are high there has been commentary to suggest the scope of directly state-backed threats will remain in-check. However, as part of due diligence, organizations who could fall within the realm of targeting if the conflict were to escalate should take note of the use of wipers and the surrounding tradecraft.

This has not limited the operations of hacktivists who have got involved in support of both sides of the conflict to cause disruption across a much broader scope of organizations. F-Secure can attest from its own data that there has been a large spike in the download of denial-of-service tooling in the regions of interest. The use of such tooling by less skilled operators can cause knock on effects to wider organizations directly or indirectly due to saturation of internet infrastructure and impact on key providers.

At the time of writing, F-Secure assesses there are five key threats for organizations to consider as a result of this developing situation:

Ransomware

The threat from ransomware is ever present; however, F-Secure assesses there is an increased likelihood that some organizations may be targeted by ransomware groups who may act in support of the Russian state. It is plausible to conclude that organizations operating in countries that have enacted sanctions against Russia, that have published messages in support of Ukraine or who have announced anti-Russian actions such as withdrawal of economic support may be targeted.

Hacktivism - Disruptive

There are widely reported DDoS attacks being conducted against organizations from both sides of the conflict. F-Secure assesses it is reasonable to assume that organizations may suffer disruption due to being directly targeted or indirectly impacted by such attacks. Those impacted to date include CNI, Finance, Telecoms, Military Supply Chain and Media organizations. In addition to DDoS attacks, there have been reports that suggest attackers have intended to delete files or disrupt systems of victims they have gained access to. It is important organizations consider these types of attacks as well as DDoS vectors when planning mitigations.

Hacktivism - Data Theft

Similar to the Hacktivism DDoS / Disruption threat there is widespread reporting of attacks being conducted against organizations in support of one side of the war or the other. There is a risk with groups such as CONTI declaring their support for the Russian state, and the escalating nature of these attacks, that more actors will become involved, and a wide range of victims be impacted by these potentially indiscriminate attacks. The difference for these types of attacks is that Data may be stolen and leaked, causing impact to the organization the data was stolen from as well as potentially the data subjects.

Insider Threat

The Russia-Ukraine conflict has brought out strong emotional and political responses from many individuals and organizations. The views on the conflict are heavily polarized between the two sides, and this kind of environment can lead to the circumstances where individuals may act to support their "side" by performing a malicious action against their employer. There has been one reported instance of this already in relation to a Russian superyacht. In addition, foreign agents may be more willing to induce insider actions by individuals against a wider range of organizations due to the increased tensions and backdrop of actively adversarial actions such as economic sanctions and armament of an opposition military force. This is mainly a risk for organizations working in CNI or politically linked organizations, though there is a risk to wider organizations as potential collateral targets. Organizations who have operations in Russia, Ukraine or service organizations who do should consider their risks from insider threats as part of this conflict.

State-Backed Threats

The use of Wiper malware has already been well documented as part of this conflict, which F-Secure assesses is likely a state-backed operation. It is possible that these type of attacks or other state-backed espionage style attacks may be conducted as part of the escalating Russia-Ukraine conflict. Disruption and intelligence gathering of information that may give one side an advantage in the ongoing conflict are likely objectives for state-backed threat actors. F-Secure assesses that these types of operations are most likely against CNI organizations in Ukraine and NATO, but that tertiary targets from organizations in those countries are plausible. However, for the majority of organizations state-backed threats are a less likely risk than the others mentioned in this report and so should not be overly focused on unless an organization clearly fits within relevant targeting criteria for these operations. Beyond traditional CNI, media organizations may be targeted as part of disinformation campaigns being conducted by state-backed actors.

F-Secure cautions organizations to not drastically change their security strategies unless they clearly fit within a high-risk targeting profile as a result of the Russia-Ukraine conflict. It is likely that for the majority of organizations they will see no impact from the conflict and should continue to execute their existing strategies and operations. For relevant organizations, the recently released US CISA report and NSA guidance provide good guidance of the range of mitigations organizations should be considering.

SANDWORM: USING NEW MALWARE CYCLOPS BLINK

SUMMARY

The United Kingdom's National Cyber Security Centre (NCSC) and United States Cybersecurity and Infrastructure Agency (CISA), National Security Agency (NSA) and Federal Bureau of Investigation (FBI) have released a joint advisory regarding the detection of a new malware named "Cyclops Blink".

The advisory discusses the use of Cyclops Blink by Sandworm, a threat actor who has previously been linked to Russia's intelligence services. Sandworm are suspected to be actively involved in espionage and to be behind the 2015 attacks on Ukraine's power infrastructure, the use of Industroyer malware in 2016, the use of NotPetya malware in 2016, attacks during the Winter Olympics in 2018 and attacks against Georgia in 2019.

Sandworm have previously used malware named "VPNFilter", with Cisco Talos publishing detailed articles describing the malware in 2018. The joint advisory states that Cyclops Blink appears to be a replacement for VPNFilter and describes it as a "large-scale modular malware framework which is affecting network devices", and states "Cyclops Blink is a malicious Linux ELF executable, compiled for the 32-bit PowerPC (big-endian) architecture. NCSC, FBI, CISA, NSA and industry analysis has associated it with a large-scale botnet targeting Small Office/Home Office (SOHO) network devices".

The report notes that Cyclops Blink was installed on WatchGuard devices and that initial access is associated to exploitation of the remote management service of WatchGuard devices, though the advisory notes Sandworm are capable or compiling the malware to target other architectures.

Cyclops Blink is modular, and therefore has a wide range of capabilities and can be updated with new abilities via its command and control server (C2). It's capabilities include system reconnaissance, file upload/download, persistence and update via C2.

The NCSC has provided a full malware analysis report and mitigation advice, including tooling and guidance provided in collaboration with WatchGuard.

F-SECURE'S INSIGHT

Sandworm are a capable Russian state-backed threat actor, who are known to engage in acts of cyber espionage which align with Russia's military and intelligence goals. Cyclops Blink is just one piece of malware, within an extensive toolkit used by Sandworm and other state-backed threat actors associated with Russia, but is being used far more broadly as a way to create a sizeable botnet. As Cyclops Blink is gaining initial access through improperly and poorly configured remote management systems, it highlights the importance of not exposing network management devices to the internet, and proper network security management.

KARAKURT: A THREAT ACTOR FOCUSED ON EXTORTION

SUMMARY

The NCC group's Cyber Incident Response Team (CIRT) has released research on a threat actor called "Karakurt" who are engaging in data theft and subsequent extortion of their victims. The threat actor was first identified in June 2021 and have self-proclaimed the name Karakurt.

The research claims that "in all cases investigated, Karakurt have targeted single factor Fortigate Virtual Private Network (VPN) servers" and that "it was observed that access was made using legitimate Active Directory credentials for the victim environment". As well as pointing out that the VPN servers attacked were not vulnerable to well-documented critical vulnerabilities in Fortigate, suggesting another method had been used to obtain the credentials.

Karakurt are described as using "living off the land" techniques and making use of legitimate tools and techniques including use of PsExec, RDP, exportation of the DNS zone, and the misuse of AnyDesk and Rclone. The use of Rclone is believed to be in relation to the exfiltration of stolen data to cloud services such as those provided by Amazon, Dropbox, Google, Mega and Microsoft; with the NCC group providing specific guidance on the detection of Rclone.

F-SECURE'S INSIGHT

While Karakurt are not thought to be exploiting well-known vulnerabilities in Fortinet VPN devices, opportunistic mass scanning for these is known to occur and exploitation of them is a recognized technique of several threat actors, highlighting the importance of patch management.

Karakurt's use of compromised credentials highlights the important of multi-factor authentication (MFA) and the use of MFA should be considered a vital security control for all external access.

Very little is known about the operators of Karakurt, but initial research would indicate they are opportunistic financially motivated cyber-criminals who focus on data theft and then extortion of victim organizations. This tactic is an increasingly common amongst cyber-criminal groups and is likely a threat that will grow in prevalence outside of the more traditional ransomware groups.

DAXIN: A CHINESE-LINKED ESPIONAGE TOOL

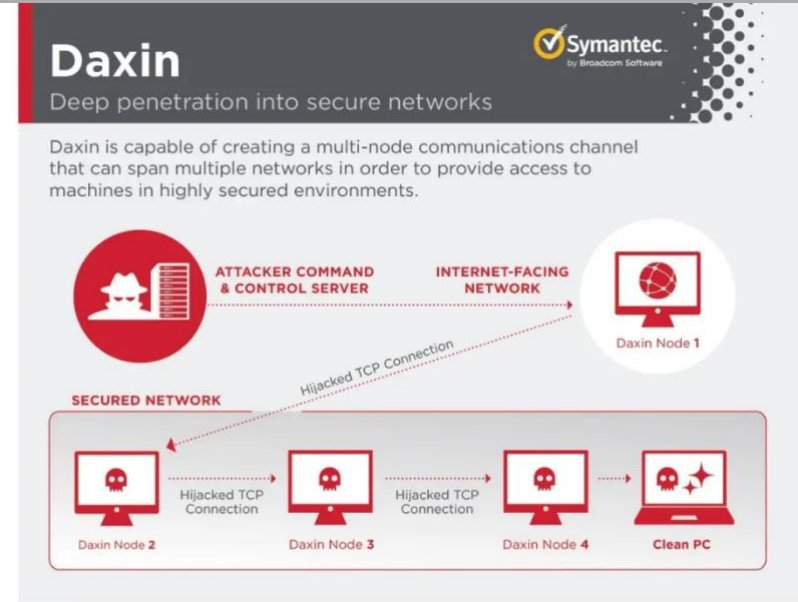
SUMMARY

Researchers at the Symantec threat hunter team have released intelligence relating to malware named "backdoor.daxin", describing it as *"...the most advanced piece of malware Symantec researchers have seen used by a China-linked actor"*.

The malware is suspected to be used to conduct espionage, with known targets including entities which would be of strategic interest to China, such as government organizations, telecommunication, transportation, and

manufacturing companies. The use of Daxin is also linked to other malware including Owprox, a trojan associated with the Chinese state-backed threat actor Chimera.

Daxin's capability includes covert communications, data gathering, and *"...exhibiting technical complexity previously unseen by such actors"*. Daxin is packaged as a Windows kernel driver and its primary capability is the hijacking of legitimate TCP/IP connections, allowing it to build a covert communication network across what would ordinarily be secure networks, and network hopping in a way that may evade firewalls and detection by analysts.



Source: Symantec Enterprise Blogs

Symantec state they are continuing to analyse Daxin and follow up technical analysis and insights will be available in the near future.

F-SECURE'S INSIGHT

Daxin's complex construction and capability are highly indicative of a state-backed malware and its usage against governments and critical infrastructure further this conclusion.

While analysis of Daxin is ongoing, it is capable of evading detection and being covertly operated. This report as well as other recent reporting of low-level state-backed malware samples indicate the continuing evolution of capability in this space. As blue team detection capabilities have drastically improved on the endpoint over the last decade, so have the tactics by high capability threat actors. These threats either attempt to blend in with legitimate activity or operate in collection blind spots of endpoint agents. Organizations with this caliber of threat actor in their threat profile should carefully consider their endpoint agent partners and the wider detection capability they may need to detect these threats.

While the use of tailor-made malware by state-backed threat actors is nothing new, Daxin does highlight the ongoing threat state-backed threats pose to organizations in key verticals.

RANSOMWARE: TRENDS AND NOTABLE REPORTS

SUMMARY

Recovery of data encrypted by Hive ransomware

A team of South Korean researchers have analysed the encryption method used by the ransomware group Hive, uncovering a way to guess the keystreams used by the threat actors, partially recovering the master encryption key. This method is reportedly able to recover around 82-98% of victims files, with the research being sponsored by the Korean government. The team have released a whitepaper of their findings.

Joint advisory on ransomware

The UK NCSC, US CISA, NSA,FBI and Australian Cyber Security Centre (ACSC) have released a joint advisory titled *"2021 trends show increased gloabilised threat of ransomware"*. The advisory highlights ongoing attacks on critical infrastructure sectors such as defence, education, energy, agriculture and technology by ransomware groups. The advisory also includes technical details regard common initial access vectors and groups tactics, techniques and

procedures, as well as suggesting mitigations and advice regarding incident response.

CONTI Leaks

As briefly discussed in our Ukraine insight, the CONTI group have suffered a breach, with their data being leaked in open source. Importantly for defenders the leaks include instruction manuals and lots of discussions on tradecraft used by the group and its affiliates. There is an excellent thread by the DFIRReport on twitter who have highlighted many of these snippets. The leaks also provide insight for defenders on how the group operates that provide useful intelligence for understanding the strategic threat these groups pose.

F-SECURE'S INSIGHT

The ransomware landscape is continually evolving with threat actors adapting their tactics, techniques and procedures over time, as well as changing their victim profile. The invasion of Ukraine has also highlighted the association between certain ransomware groups, states and the threat they present to critical infrastructure, and is backed up by the recent joint advisory published by the NCSC suggesting national critical infrastructure across the US, UK and Australia is constantly being impacted by these threats.

The CONTI leaks are likely to be useful data for improved detection by many organizations and also potentially lead to law enforcement action with many of the members being publicly doxed since the leak became public. CONTI have shown long term resilience in their operations and so we assess that is unlikely this will stop their operations, but may force a slight break while they retool and configure their infrastructure to be secure and to harden it to future disruption.

OTHER NOTABLE HIGHLIGHTS IN BRIEF

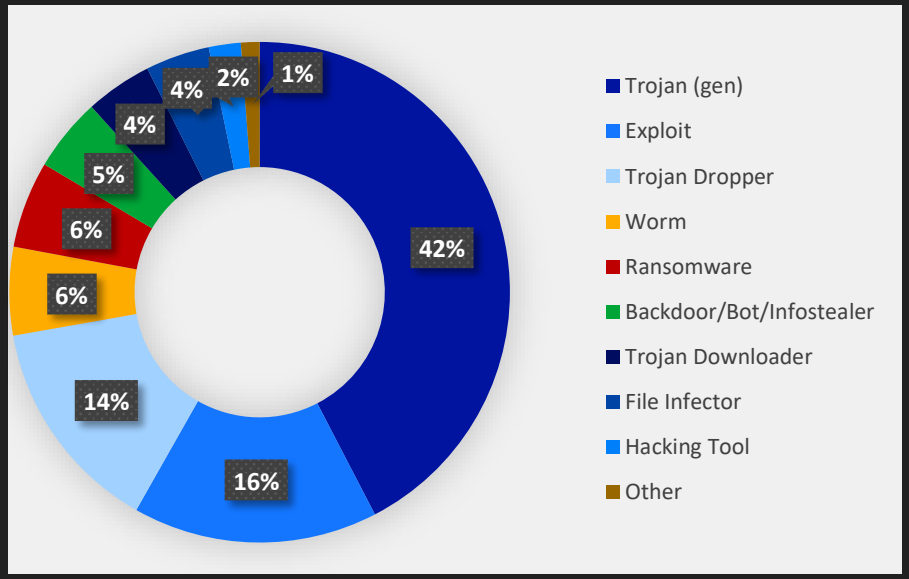
- Researchers at Pangu Lab's have released a technical paper on a Linux backdoor they are calling BVP47. The researchers have linked this activity to the Equation Group, who is reportedly a US based threat actor.
- Attacks on the Taiwanese financial sector are being attributed to the Chinese state-backed threat group APT10.
- Hackers have reportedly stolen $1.9 million from the South Korean cryptocurrency platform KLAYswap, following a successful Border Gateway Protocol (BGP) hijack on third-party infrastructure.
- A currently unattributed cyberattack on Vodafone Portugal has reportedly disrupted a number of their services.
- According to analysis by Microsoft, a Mac Trojan called "UpdateAgent" is continually being developed and updated with new techniques and capabilities.
- The company behind software suite Zimbra have released a hotfix and guidance due to a zero-day vulnerability within its software.
- Huntress Labs have identified a DPRK threat actor targeting Nuclear think tanks using the BABYSHARK malware family
- The LAPSU$ threat actor has reportedly breached NVIDIA and after a failed extortion attempt leaked their data, which includes some signing certificates that have since been used to sign malicious files
- CISA have released an alert highlighting Iranian state-backed activity that has been targeting government and communication networks globally
- Dragos have released their yearly report, that provides an excellent summary of the threats within the ICS space

F-SECURE THREAT DATA HIGHLIGHTS

MALWARE TYPES

On the malware front, for February various exploits have been the most detected threats followed by droppers.

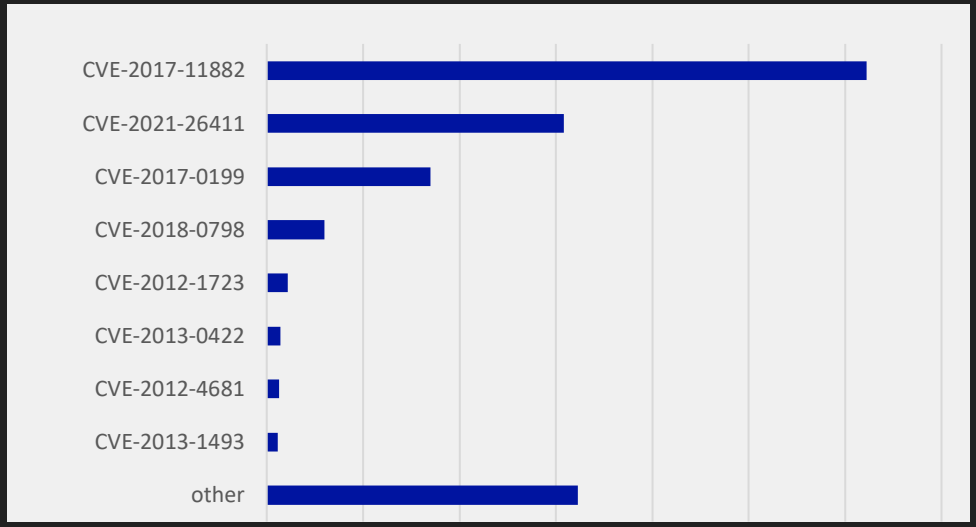
Already in January, ransomware has been lower on the list and continues so throughout February.



EXPLOITS

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker.
CVE-2021-26411 an internet explorer memory corruption vulnerability which follows at the second place. This vulnerability is exploited by malicious websites.

During February CISA added multiple CVEs to the list of vulnerabilities exploited in the wild. These include vulnerabilities in Windows and Office as well as some 3rd party software.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

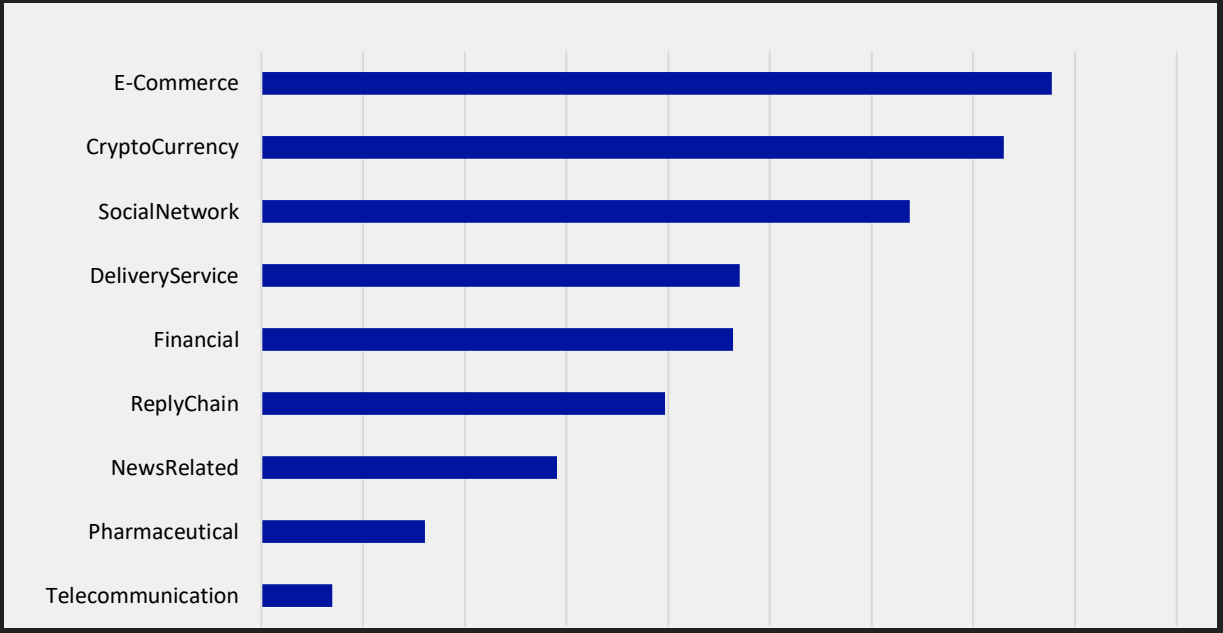


EMAIL THREATS

Cryptocurrency and e-commerce themes dominate the spam landscape. Towards the end of February, we have observed exploitation of the conflict in Ukraine by financially driven cybercriminals.

While there are legitimate options to send monetary aid to Ukraine, criminals rush to seize this opportunity to scam people over email. These spam emails contain requests for donations for Ukraine or are starting a traditional “wire fraud” scam under the Ukraine theme.
Ukrainian government has started accepting cryptocurrency donations which may make these fraudulent cryptocurrency-based fundraising seem less suspicious.

Some other observed exploitation of the conflict includes capitalizing on Ukraine themed goods and advertisement with spam campaigns and unsolicited financial advice on the market reactions to the conflict. These similar scams and activity are visible on other mediums as well such as various social media platforms. The activity is not very prevalent as of now but is likely to increase if the conflict drags on.



F-Secure®

f-secure.com/ | twitter.com/fsecure | linkedin.com/f-secure-corporation