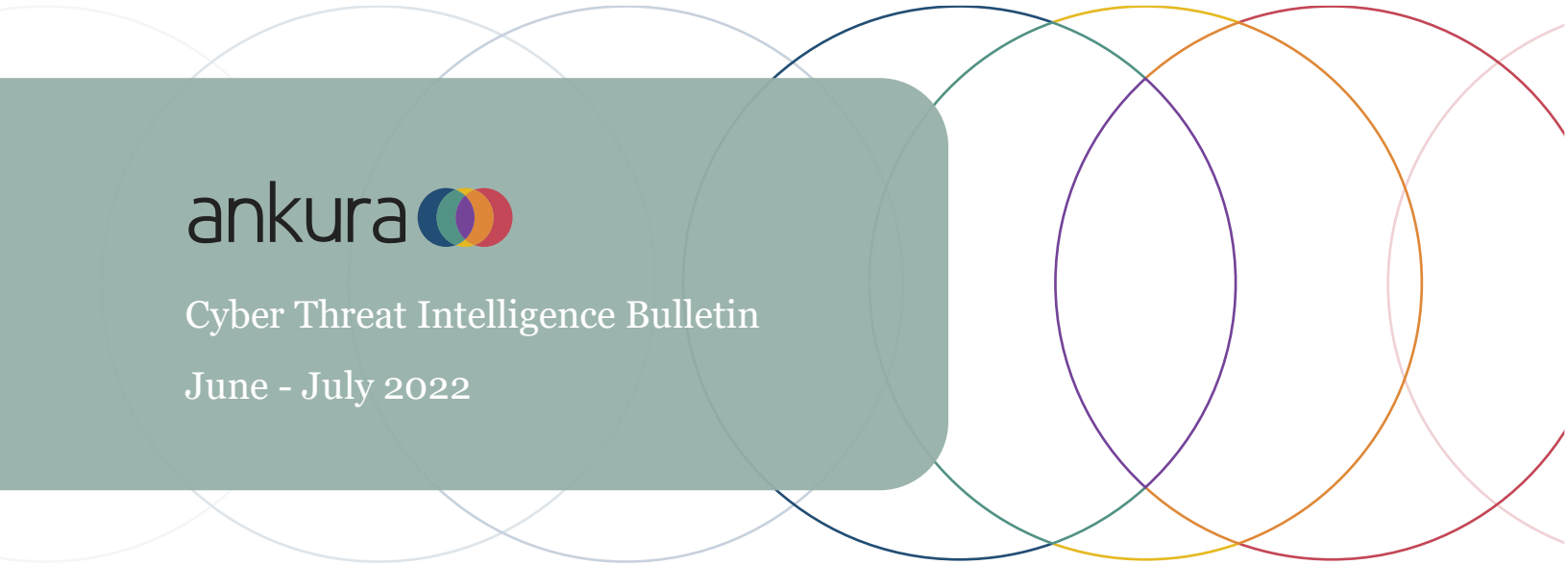

ankura

Cyber Threat Intelligence Bulletin

June - July 2022

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

TABLE OF CONTENTS

Executive Summary

Ankura's Cyber Threat Investigations and Expert Services (CTIX) team has compiled details of current cyber trends within the last sixty (60) days. This summary is intended to provide a medium depth of knowledge to high-level executives, technical analysts, and everyday readers who are looking to gain a deeper understanding of current, global threats.

This report will discuss the following in detail:

- Sweden and Finland joining NATO, and the cyber response by Russia.
- The recent evolution of ransomware groups and their tactics, techniques, and procedures (TTPs).
- A joint advisory released by the directors of the FBI and MI5, warn of the rapid increase in Chinese-affiliated threat actor behavior over the past four (4) years.
- The Biden administration introduced the Quantum Computing Cybersecurity Preparedness Act, and the National Institute of Standards of Technology (NIST) unveiled state-of-the-art encryption tools engineered to defend against future quantum computing attacks.
- The TTPs of the up-and-coming Russian-affiliated "Killnet," threat group, as they conduct malicious cyber campaigns against Ukrainian targets in support of the Russian military invasion.

RUSSIA SETS ITS SIGHTS ON NEW TARGETS AS SWEDEN AND FINLAND JOIN NATO

- Finland and Sweden have both experienced a lower volume of cyberattacks than expected after filing applications to join NATO.
- Both countries have integrated well into NATO cyber defense initiatives and shown their own progress in the field.
- Targeted political cyberattacks are being used in an attempt to dissuade the Scandinavian countries from cooperating with the broader Western coalition.

Summary

With the ongoing Russian invasion of Ukraine and the ever-evolving proxy war between NATO and Russia, adding new players to the field is likely to cause new actions from both sides. With both Sweden and Finland officially agreeing to join NATO and beginning the Ascension Protocols, the focus has shifted to the new frontline in Scandinavia. With Norway already being an established member of NATO and heavily backing Sweden and Finland's entrance to the alliance, the Scandinavian block now poses a large and renewed threat to Russian interests and security on its European border. While unable to exert influence and threats via traditional military means against these countries, cyberattacks prove to be an effective way for Russia to voice her displeasure with the new status quo this brings about. Interestingly, CTIX analysts have observed a similar number of cyberattacks against Sweden and Finland since their applications to NATO were filed, when compared to the level of attacks in the months immediately prior to the formal filing for membership. Finnish Cyber Security Centre (CSC) Director General Sauli Pahlman reported that "the situation had has remained stable in recent weeks," and that while weekly reports to the CSC have jumped

from twenty-one (21) to thirty-six (36) since applying to NATO, Pahlman stated that it was "…by no means an exceptional amount…".[1]

There are a multitude of factors that can play into this subversion of expectations when many were expecting an endless onslaught of attacks against the Scandinavian nations. One (1) large factor for this could be the recent improvements of Finnish cybersecurity capabilities combined with integration into the NATO cyber sphere. In late April 2022, both Finland and Sweden participated in the Locked Shields NATO exercise which involved a "live fire," cybersecurity response competition between teams from many NATO countries and direct NATO allies. In a show of force, Finland's team had the most effective response to the exercise, placing first out of twenty-four (24) teams. This ranking demonstrated Finland's ability to quickly respond to real cyber threats and integrate itself into the broader defensive structure.[2]

While the Scandinavian countries seem to have effectively come together to repel many cyberattacks, there are a few examples of incidents that managed to circumvent the defensive perimeter. One (1) example includes the attack against Finnish websites during a Parliament conference with Ukrainian President Zelensky in late April 2022. This was a DDoS attack that targeted the Finnish Foreign and Defense ministries websites, making them inaccessible for several hours during the meeting. Finland, however, managed a rapid recovery of services.[3] Although the Finnish government has not directly attributed this attack to entities backed by the Russian state, the timing and target heavily suggest Russia or Russian-backed groups as the culprit.

Norway has also had its share of cyberattacks in recent months despite already being integrated into the NATO structure as a founding member of the alliance. This could be due to Norway's past and current support of its Nordic neighbors and their acceptance into NATO. In late June, Norway experienced a large-scale DDoS attack against multiple websites and services after blocking Russian goods and donating military equipment to Ukraine. The websites targeted in this attack were found to come from a target list posted by "Legion – Cyber Spetsnaz RF" on their Telegram channel.[4]

[1] https://yle.fi/news/3-12464507
[2] https://thestack.technology/finland-wins-nato-cyber-exercise-locked-shields/
[3] https://www.cybersecurityintelligence.com/blog/finland-hit-by-cyber-attack-6238.html
[4] https://www.bleepingcomputer.com/news/security/russian-hacktivists-take-down-norway-govt-sites-in-ddos-attacks/

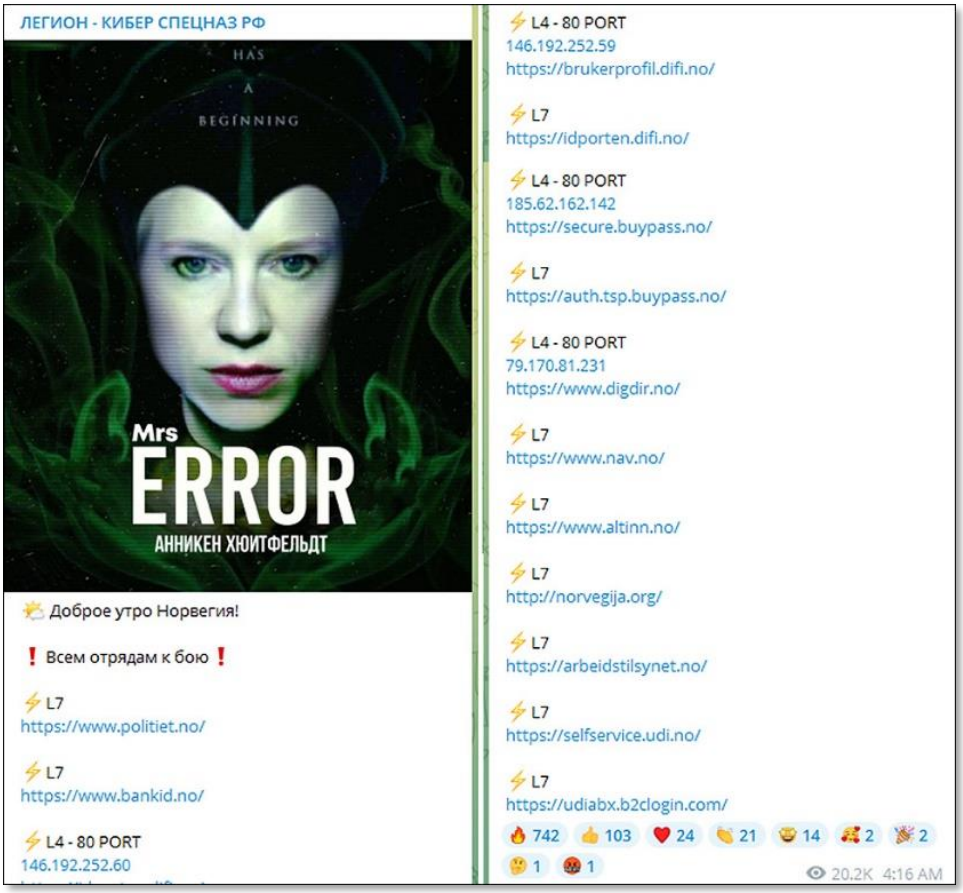

Figure 1: Target list on "Legion – Cyber Spetsnaz RF"'s Telegram channel

The connecting factor between many of the cyberattacks against Scandinavian countries is their apparent lack of sophistication, either by executing broad-spectrum DDoS attacks or basic ransomware schemes. At least for the moment, the majority of these attacks seem to be political statements from Russia and Russian groups. This is possibly due to the guarantees of defense Finland and Sweden have already received from countries in NATO, specifically the United States and the United Kingdom. Either way, it is likely that this is not the full might of Russia's cyber ability and is merely meant to pester these countries on top of the political rhetoric directed at them. Ankura will continue to monitor threats against the incoming NATO allies and evolving cyberattacks connected to the war in Ukraine.

ADVANCEMENTS IN RANSOMWARE ADMINISTRATION

- Ransomware groups are evolving from small groups to large organizations.
- New techniques, such as a searchable database, are putting more pressure on victims to pay a ransom.
- LockBit is increasing their security with a bug bounty program and monetizing data before it is publicly released.
- ALPHV and LockBit's organizational growth allows the groups to demand ransoms up to $2.5 million and $5 million.

Summary

Ransomware has become an increasingly popular tool used by financially motivated cyber criminals for many years now. Threat actors utilizing ransomware boomed between 2015 and 2017 when, according to Verizon's Data Breach Investigation Report, ransomware incidents increased from less than 5% of attacks in 2015[5] to 38% in 2016[6] and jumped into the number one (1) spot in 2017[7] accounting for close to 50% of all crimeware incidents. Since the surge, threat actors utilizing ransomware have developed new techniques to demand more money for initial ransoms. In 2017, most ransomware attacks only encrypted data and demanded a ransom in exchange for a decryption key.[8] This led to issues as the ransomware being developed at the time was often bug-ridden. Almost half of the organizations who paid the demanded ransoms could not recover their data using the decryption keys provided by the threat actors due to faulty encryption or decryption techniques.[9] Organizations began to take notice that paying the ransom did not guarantee the recovery of their data. This led to less than 40% of victims paying ransoms during that time since 50% of organizations could recover their encrypted data without paying the ransom, likely through data backups.[10]

Ransomware groups needed another attack vector, and in 2019 they began utilizing double extortion in their attacks. A double extortion ransomware attack is when threat actors not only encrypt the victim data, but also exfiltrate it to further pressure the victims to pay the ransom, or risk having their data leaked/sold. As identified by CrowdStrike, the threat actor OUTLAW SPIDER, well known for the "RobinHood" ransomware, posted the data exfiltrated from the U.S. City of Baltimore following the city's denial of the compromise of personal information. OUTLAW SPIDER stated they would remove the data if the city paid the demanded ransom.[11] Though this technique was ineffective in this case, other ransomware groups began creating leak sites, most notably the Maze ransomware group who popularized and refined the technique, turning it into the threat we know today. During this time, ransomware groups developed an identity by creating blogs and social media accounts that announced their "clients". In addition to this, ransomware groups began using DDoS attacks targeting victims' public-facing infrastructure. These new developments led victims to pay the ransoms more than 80% of the time in 2021.[12]

Ransomware threat actors have not stopped developing new techniques. ALPHV, the first ransomware organization to develop their malware in the Rust programming language, has created a searchable database that allows the employees and customers of compromised organizations to search for their data.

---

[5] https://www.verizon.com/business/resources/reports/data-breach-investigation-report_2015.pdf
[6] https://www.verizon.com/business/resources/reports/DBIR_2016_Report.pdf
[7] https://www.verizon.com/business/resources/reports/2017_dbir.pdf
[8] https://docs.broadcom.com/doc/istr-ransomware-2017-en
[9] https://cyber-edge.com/wp-content/uploads/2021/03/CyberEdge-2018-CDR.pdf
[10] https://cyber-edge.com/wp-content/uploads/2021/03/CyberEdge-2018-CDR.pdf
[11] https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
[12] https://thycotic.com/resources/ransomware-survey-and-report-2021/

This new technique increases pressure on the victim organization, as people can confirm whether they are included in the breach and hold the compromised organization accountable. Following the release of this database, LockBit, a threat group operating since 2019[13] and considered one of the largest ransomware-as-a-service (RaaS) organizations today[14], implemented a similar feature to their leak site allowing users to search for companies victimized by the group. The search functionality is much less advanced than ALPHV's and only allows searching based on the company name. Alongside their searchable database of victims, ALPHV has increased their initial ransom demand to a reported $2.5 million, though most organizations likely negotiate this down to a more affordable price.[15]

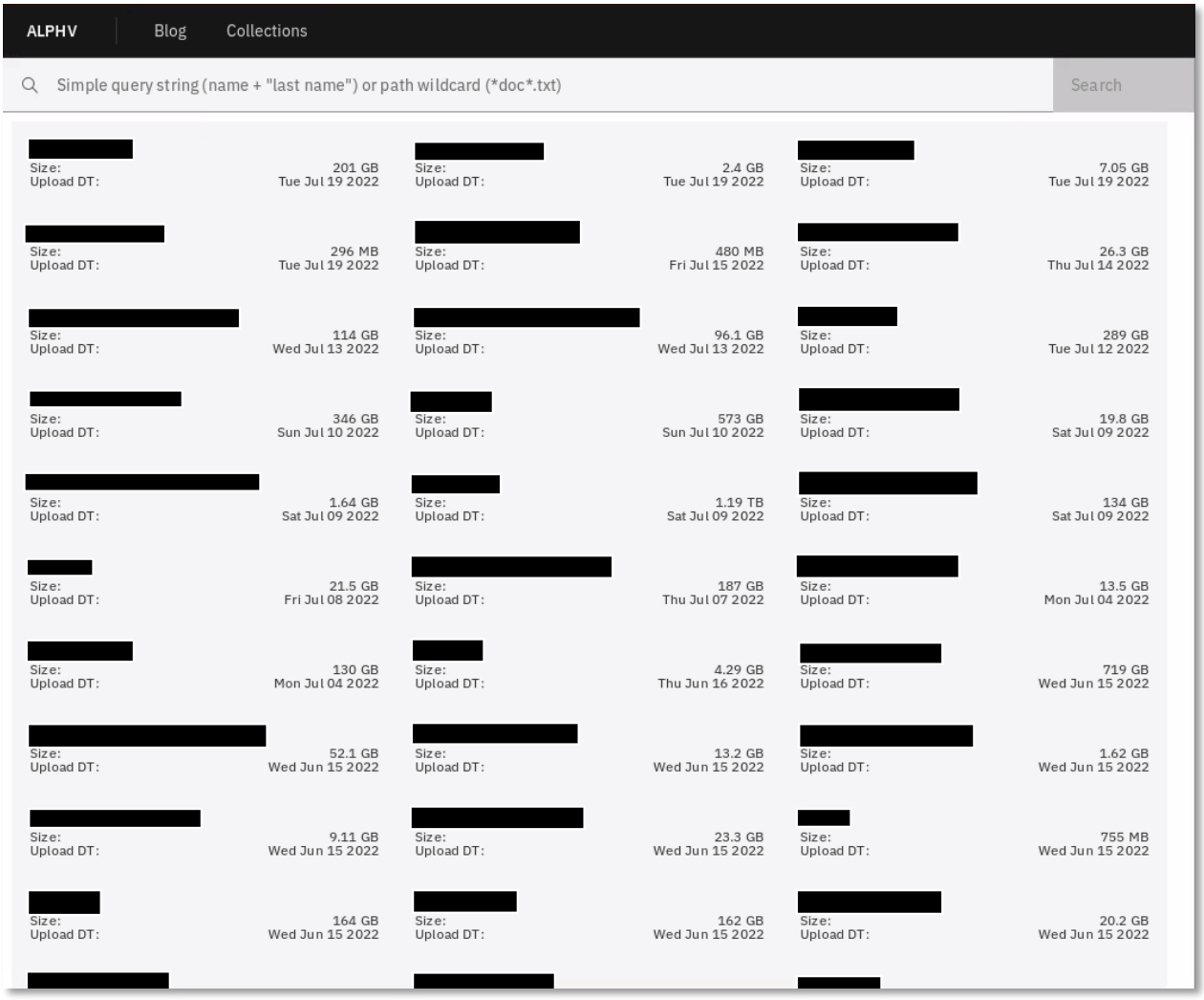

Figure 2: ALPHV Database Search Site

With the development of these new techniques and the financial gain brought with them, ransomware groups have expanded from small gangs to large organizations. Internally, their leaders began to operationalize their practices. While this has been speculated for years, it was confirmed following the leak

[13] https://arstechnica.com/information-technology/2020/05/lockbit-the-new-ransomware-for-hire-a-sad-and-cautionary-tale/
[14] https://blog.sekoia.io/sekoia-io-mid-2022-ransomware-threat-landscape/
[15] https://resecurity.com/blog/article/blackcat-aka-alphv-ransomware-is-increasing-stakes-up-to-25m-in-demands

of Conti's internal documentation.[16] Following Conti's February 2022 announcement for the support of Russia in their conflict with Ukraine, a Ukrainian group member leaked two (2) years' worth of chat logs and internal documents.[17] The leak detailed how the Conti ransomware group has departmentalized their members in a similar fashion as legitimate organizations, creating a human resources department to hire new employees and create budgets and staff schedules.[18]

The newest development comes from the LockBit ransomware group. The threat group updated their RaaS operation to "LockBit 3.0". With this update, LockBit has introduced the first bug bounty program that has been established by a ransomware group.[19] Bug bounty programs allow organizations to enlist the help of freelance ethical hackers to uncover vulnerabilities in the business's website and products. This is extremely useful for organizations as it enables them to patch critical vulnerabilities before a threat actor can exploit it. LockBit's program offers rewards ranging from $1,000 to $1 million for "all security researchers, ethical and unethical hackers on the planet" to submit bug reports for various categories such as web site vulnerabilities, encryption/decryption bugs, and more.[20]:

The creation of this bug bounty program allows LockBit to tap into a resource of security researchers and hackers. While the group could hire employees to achieve the goals outlined in the bug bounty categories, like most organizations, it is often easier and cheaper to outsource these efforts.

In addition to the bug bounty program, LockBit has implemented the ability for anyone to pay to extend a victim's timer (giving more time for negotiations), destroy the data the ransomware exfiltrated, or download the data before it is publicly available. This new feature simply gives another way for LockBit to extract more money out of victims while negotiations are ongoing.

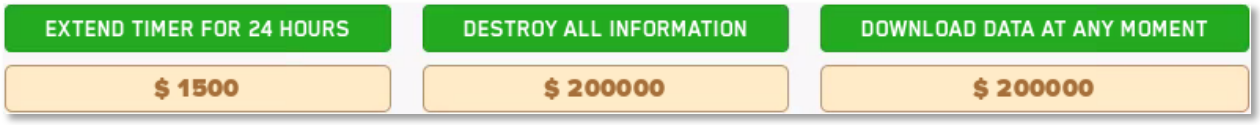

Figure 3: An Example of LockBit's Prices Before Posting Data

Ankura CTIX analysts recently discovered a new technique being utilized by LockBit. In a recent leak, LockBit publicly posted previously private negotiation chat logs to add pressure to the victim company. This is a new development never before seen employed by LockBit or any other ransomware groups. To read more about this discovery and the circumstances surrounding it, refer to the report "LockBit Implements New Technique by Leaking Victim Negotiations."[21]

It is not new for criminal groups to organize and begin to mimic the businesses they attack. These developments in ransomware threat actors signal the ongoing evolution of cybercriminals. The groups' internal administration continues to grow alongside their TTPs used during attacks. As these groups thrive with little resistance from law enforcement, they will continue to pose problems for organizations around the world.

---

[16] https://www.techtarget.com/searchsecurity/news/252514047/Conti-ransomware-source-code-documentation-leaked
[17] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/
[18] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
[19] https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/
[20] https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/
[21] https://angle.ankura.com/post/102htog/lockbit-implements-new-technique-by-leaking-victim-negotiations

RECENT ACTIVITY SURROUNDING QUANTUM COMPUTING AND ITS SECURITY RISKS

- Quantum computing is a security risk to society at large for its potential ability to break all traditional encryption.
- For the last six (6) years, the United States federal government has put efforts towards combating the risks to information technology by quantum cryptography.
- Within the last month, the United States National Institute of Standards of Technology (NIST) has revealed four (4) encryption tools designed to "withstand the assault of a future quantum computer" and the "Quantum Computing Cybersecurity Preparedness Act" has been introduced by the Senate.

Summary

The United States' Federal Government has had its eye on quantum computing for at least six (6) years and has published significant updates in the last few months.[22] A quantum computer is "a computer that uses the collective properties of quantum states to perform calculations."[23] Quantum computing is seen as a major risk to overall security as it could "break classical encryption that underpins financial stability and the global economy."[24] Tasks that would take the most powerful supercomputer in the world years would take a quantum computer hours to complete. In theory, a quantum computer could be able to break 2048-bit RSA encryption in under eight (8) hours while the world's fastest supercomputers would require 300 trillion years to complete the same task.[25] This drastic speed difference could cause major problems around the globe, as information that is in a secure state today could be at risk in the future.

[22] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[23] https://www.hassan.senate.gov/imo/media/doc/mir22641pdf.pdf
[24] https://cybernews.com/security/dangers-of-quantum-computing-from-new-style-warfare-to-breaking-encryption/
[25] https://cybernews.com/security/dangers-of-quantum-computing-from-new-style-warfare-to-breaking-encryption/

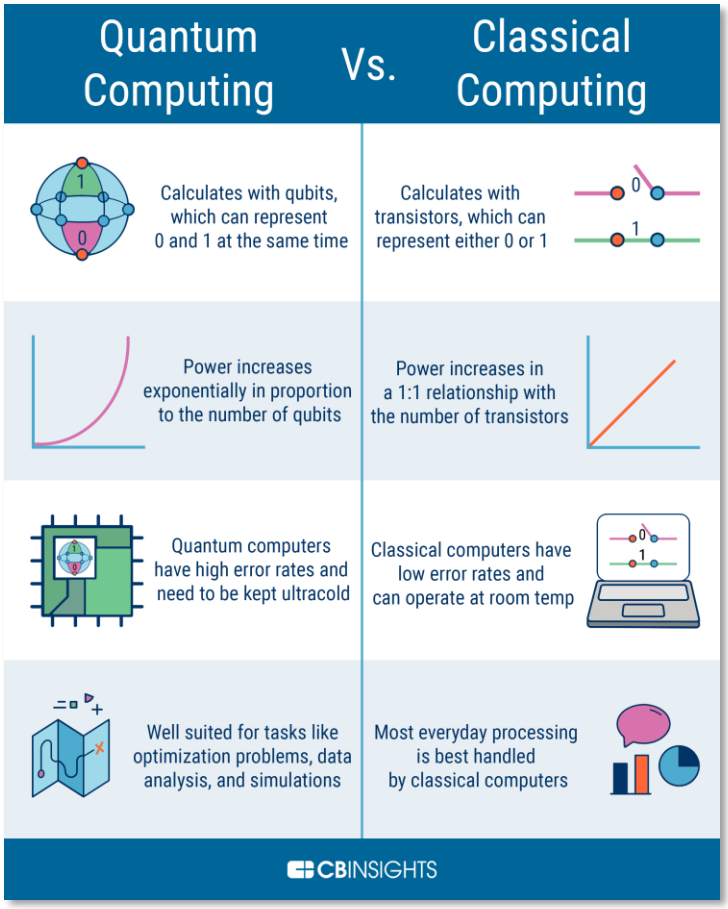

Figure 4: Comparison between quantum computing and classical computing[26]

In December of 2016, NIST made its first formal and public step towards combating the risk of quantum computing against the country's information technology, despite practical quantum computers not having been built yet. NIST announced the "Call for Proposals for Post-Quantum Cryptography Standardization" in the Federal Register, which called for "the world's cryptographers" to send proposed algorithms, methods, and strategies to the agency by November 30, 2017.[27] NIST mathematician Dustin Moody emphasized that the concern was regarding new algorithms for public key cryptography and specifically to replace three (3) NIST cryptographic standards and guidelines "that would be the most vulnerable to quantum computers": FIPS 186-4, NIST SP 800-56A, and NIST SP 800-56B[28]. These three (3) standards "deal with encryption, key establishment and digital signatures, all of which use forms of public key cryptography."[29] This announcement also ensured an in-depth analysis of submitted proposals culminating in approximately three (3) to five (5) years.

National Security Memorandum (NSM-10) Released

On May 4, 2022, the Biden administration published a national security memorandum (NSM) regarding government agencies mitigating all risks to US national security posed by cryptanalytically relevant quantum computers (CRQC). The NSM's specific purpose is to identity "key steps needed to maintain the Nation's

[26] https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/
[27] https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information
[28] https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information
[29] https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information

competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation's cyber, economic, and national security."[30] It detailed that a CRQC will be capable of breaking "much of the public-key cryptography used on digital systems across the United States and around the world" which poses the following potential risks[31]:

- "Jeopardize civilian and military communications"
- "Undermine supervisory and control systems for critical infrastructure"
- "Defeat security protocols for most Internet-based financial transactions"

In order to combat these risks, the White House is promoting several leadership objectives for the United States. These objectives include pursuing a "whole-of-government and whole of society strategy to harness the economic and scientific benefits of QIS, and the security enhancements provided by quantum-resistant cryptography," seeking to "encourage transformative and fundamental scientific discoveries through investments in core QIS research programs," seeking to "foster the next generation of scientists and engineers with quantum-relevant skill sets, including those relevant to quantum-resistant cryptography."[32] An additional objective includes promoting "professional and academic collaborations with overseas allies and partners", which is noted as "essential for identifying and following global QIS trends and for harmonizing quantum security and protection programs."[33]

The NSM also calls for mitigations for the potentially vulnerable public standards utilizing public-key cryptography. One (1) current goal presented consists of United States agencies prioritizing "the timely and equitable transition to cryptographic systems to quantum-resistant cryptography," and "mitigating as much of the quantum risk as is feasible" by 2035.[34] An additional goal is publicizing technical standards for specific jurisdictions by 2024. Action item timelines are noted in NSM-10 as well.

First Group of Quantum-Resistant Tools Revealed

On June 5, 2022, NIST revealed the first group of encryption tools that are designed to "withstand the assault of a future quantum computer" that could potentially "crack the security used to protect privacy in the digital systems we rely on every day – such as online banking and email software."[35] The chosen algorithms are designed for two (2) main tasks:

1. General encryption, which is used to protect information exchanged across a public network.

---

[30] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[31] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[32] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[33] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[34] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[35] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

2. Digital signatures, which are used for identity authentication.

The agency selected the "CRYSTALS-Kyber" algorithm for general encryption and three (3) algorithms for digital signatures to be considered for inclusion: "CRYSTALS-Dilithium", "FALCON", and "SPHINCS+".[36] NIST specified that the four (4) algorithms were created by experts collaborating from multiple countries and institutions. The four encryption tools are expected to be finalized in approximately two (2) years, becoming the post-quantum cryptographic standard. NIST also stated that four (4) additional algorithms designed for general encryption are currently under consideration to be included in the new cryptographic standard once it is finalized in roughly two (2) years.

Quantum Computing Cybersecurity Preparedness Act Introduced

On July 21, 2022, legislation titled the "Quantum Computing Cybersecurity Preparedness Act" was introduced by Senators Maggie Hassan (D-N.H.) and Rob Portman (R-Ohio). The legislation noted the following ideas according to Congress:

- Cryptography is "essential for the national security of the United States and the functioning of the economy of the United States."[37]
- The encryption protocols that are widely used today "rely of computational limits of classical computers to provide cybersecurity."[38]
- Quantum computers have the potential to "push computational boundaries" that would enable currently unsolvable problems (such as integer factorization) to become solvable, which would impact encryption.[39]
- The current quantum computing progression could allow for "adversaries of the United States to steal encrypted data today using classical computers and wait until sufficiently powerful quantum systems are available to decrypt it."[40]

This act's goal is "to encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes."[41] The act would also direct the Office of Management and Budget (OMB) to begin taking steps to stimulate the technology migration needed in the future.

Mitigations

The United States is progressing at a steady rate to adhere to the intended timeline. Additional legislation created to combat the security risks associated with quantum computing will be introduced and accepted within the next ten (10) years. To prepare for future standards and regulations, organizations can inventory their systems now for all applications that are currently using public-key cryptography. Once the impacted applications are collected, it is advised that the following characteristics[42] be determined:

---

[36] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[37] https://www.hassan.senate.gov/imo/media/doc/mir22641pdf.pdf
[38] https://www.hassan.senate.gov/imo/media/doc/mir22641pdf.pdf
[39] https://www.hassan.senate.gov/imo/media/doc/mir22641pdf.pdf
[40] https://www.hassan.senate.gov/imo/media/doc/mir22641pdf.pdf
[41] https://www.hassan.senate.gov/imo/media/doc/mir22641pdf.pdf
[42] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

- Identify the level of sensitivity of the information that is being protected.
- Identify the entities owning, manufacturing, and supplying cryptographic hardware, software, or processes.
- Deduct if an application can be programmatically updated to meet future security standards.
- Identify how long the applications will continue to be supported by the organizations maintaining them before their expected end-of-life.
- Determine which handshake key-exchange protocols are currently in use.
- Determine the impacts to intellectual property stemming from the new migration.

It is not recommended that organizations implement new algorithms into their systems quite yet, as the reviewed algorithms may change prior to the finalization of NIST's post-quantum cryptographic standard and the requirement to adjust is not present as of this publication.

FBI AND MI5 PUBLICLY ADDRESS GROWING CPC CYBERSECURITY CONCERNS

- Businesses must be proactive when protecting their intellectual property and information from an increasing Communist Party of China cyber threat.
- China has expanded its state-sponsored hacking program to be the largest in the world.
- The continued buildup of CPC cyber espionage efforts suggests that China wants to increase its influence across the globe.

Summary

On July 6, 2022, MI5 Director General Ken McCallum and FBI Director Chris Wray issued a joint address for the first time in history. The reasoning behind this unprecedented move was to provide a warning on the "growing threat posed by the Chinese Communist Party to UK and US interests."[43] Over the course of the past few years, Communist Party of China (CPC) has exponentially increased its cyber espionage activity to levels never before seen. MI5 reported that it has conducted seven (7) times as many investigations as compared to 2018.[44] As a whole, the goal of most of the CPC's cyber espionage appears to be to gain a competitive advantage over western countries in the tech industry. However, cyber espionage is not the only strategy used by the CPC to gain an advantage.

Last year, Chinese intelligence officer Shu Yenjoon was convicted in a United States court on charges of economic espionage and theft of trade secrets from the US aviation sector.[45] Shu was also active in Europe, targeting the aerospace sector and proving to be a prime example of China utilizing embedded state agents to commit theft of information without resorting to cyberattacks. Cyber espionage isn't always necessary; sometimes Chinese companies will use business partnerships as a trojan horse. One example of this strategy involves Smith's Harlow, a UK-based precision engineering firm that entered a deal with Futures Aerospace, a Chinese firm. After Futures paid £3M for quality control procedures and training courses for the first three (3) technology transfers, they acquired as much valuable intellectual property as they could, and then abandoned the deal. [46]

This aggressive behavior by China indicates just how motivated they are on becoming the lead superpower in the world, and over time security researchers have observed a rapid expansion of Chinese state-sponsored hacking programs. CPC's investment into the government's hacking program has evolved into a program "bigger than that of every other major country combined," according to the FBI Director Chris Wray.[47] In response to these allegations, a spokesperson from the Chinese embassy stated, "the allegations against China by U.S. and UK intelligence officials are completely groundless and the so-called cases they listed are pure shadow chasing."[48] The spokesperson also suggested that the UK and US "abandon the Cold War mentality which has long gone out of date" as well as "stop spreading [the] 'China threat'."[49] However, China seems to maintain its cold war mindset, reportedly interfering in other countries for its own agenda. In 2022, the Chinese government allegedly targeted New York Congressional candidate Xiong Yan, who was involved in the 1989 protest in Tiananmen square and fled China as a political refugee

[43] https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi
[44] https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi
[45] https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi
[46] https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi
[47] https://www.reuters.com/world/heads-mi5-fbi-give-joint-warning-growing-threat-china-2022-07-07/
[48] https://www.reuters.com/world/heads-mi5-fbi-give-joint-warning-growing-threat-china-2022-07-07/
[49] https://www.reuters.com/world/heads-mi5-fbi-give-joint-warning-growing-threat-china-2022-07-07/

in 1992.[50] The Chinese government secret police reportedly hired private investigators to discredit him and even discussed plans to physically assault him or stage a car crash.

Directors McCallum and Wray closed their address by warning that while MI5 and the FBI are increasing their investigations into Chinese threats, it may not be enough. Private businesses must remain vigilant against this looming threat when protecting their interests along with efforts by the UK and US governments. To help protect the interests of these companies, the US is passing the "Better Cybercrime Metrics Act"[51]. This act encourages local law enforcement to report incidents of cybercrime to the FBI to build a database of cybercrimes. The data collected will be available to law enforcement agencies seeking to track down cybercriminals. The UK is taking similar measures with the "National Security Bill" currently before Parliament. This bill will be updating the core espionage offenses and tackle covert influencing against democracy. Threats not just to national security but to privately owned intellectual property are on the rise. It's only logical that the UK Parliament draws new lines for the 21st century. That being said, efforts to stop cybercrime by the government alone will not be enough to mitigate Chinese cyber risks, and the intelligence agency directors urge private companies to implement as well as maintain their own cybersecurity practices. Additional recommendations to organizations include discussing the risk of Chinese cyber activity to their infrastructure, creating a thoughtful security culture at all levels, and consistently updating all systems.

[50] https://www.reuters.com/world/heads-mi5-fbi-give-joint-warning-growing-threat-china-2022-07-07/
[51] https://www.congress.gov/bill/117th-congress/house-bill/4977

THREAT ACTOR OF THE MONTH

- Killnet is a rising threat organization openly aligned with Russia.
- Killnet targets those who assist Ukraine throughout the conflict with significant DDoS attacks and general compromises.
- Activity from the organization is predicted to rise as the conflict continues and more hacktivist supporters assist the Killnet organization.

Summary:

Since the start of the Russia-Ukraine invasion in February, the threat landscape has significantly changed, and threat actors globally have taken stances with their respective sides. One (1) rising threat organization that has made significant movements surrounding the conflict in recent weeks is Killnet. This threat organization has compromised assets that either align with Ukraine or participate in active sanctions against the Russian state. Over the past weeks, Killnet threat actors have targeted Lithuania in retaliation for Russian sanctions, Norway with significant distributed denial-of-service (DDoS) attacks, and several other countries siding with Ukraine. Recently, Killnet has started its ongoing cyberwar with ten (10) countries including the United States and United Kingdom.

Killnet was originally a smaller threat organization that utilized a tool called “Killnet” to perform their DDoS attacks, often hitting smaller targets prior to the global conflict. Since the first Russian soldier crossed into Ukraine, Killnet grew from a small threat group to a rising hacktivist organization[52]. Under the Killnet umbrella lies an elite squad of Killnet threat actors called the “Cyber Special Forces RF”, otherwise known as “Legion”, who perform extensive DDoS attacks against its targets.[53] Recruitment for the organization occurs through the group’s Telegram channel, primarily in search of actors with advanced knowledge in penetration testing, DDoS attacks, phishers, and general hacking capabilities. Several squadrons of hackers have already been crafted by the Legion group and are code named “Kratos”, “Rayd”, and “Sakurajima” among others. Each squadron is responsible for conducting DDoS attacks against a selected target or a provided region, for which individual attackers have free reign to attack any entity they see as a qualifying target.

[52] https://intel471.com/blog/killnet-xaknet-legion-ddos-attacks
[53] https://www.digitalshadows.com/blog-and-research/killnet-the-hactivist-group-that-started-a-global-cyber-war/

Figures 5 & 6: Recruitment postings for Killnet[54] and Killnet's Legion group[55]

Indications of cyberattacks tied to Killnet have been identified throughout the European region, including Romania, Norway, Lithuania, Italy, Latvia, Moldova, and the Czech Republic. Recently, Lithuania has been a key target for the Killnet organization. In retaliation for geopolitical sanctions against the Russian state and the halting of transportation services through the country (Lithuania), attackers launched significant DDoS attacks against the country rendering secured data networks, the State Tax Inspectorate, the Migration Department, as well as several other government entities inaccessible. After the initial wave of DDoS attacks, Killnet unleashed additional attacks against the Vilnius, Kaunas, and Palanga airports, the Central State Archive, the Supreme Administrative Court, and several organizations throughout the telecommunications industry within the region.

Other significant attacks by the Killnet organization since the start of the Russia-Ukraine conflict include, but are not limited to:

- Czech Republic: Several websites were taken down throughout the government, financial, telecommunications, and transportation industries.
- Italy: Several websites originating with the Istituto Superiore di Sanità and the Automobile Club of Italy were taken offline for several hours.
- Norway: DDoS attacks against several Norwegian organizations.

[54] https://www.pwndefend.com/2022/05/18/killnet-area-they-really-a-threat/
[55] https://www.digitalshadows.com/blog-and-research/killnet-the-hactivist-group-that-started-a-global-cyber-war/

- Estonia: Attacks targeting government and telecommunications sectors.
- United States: Knocked the United States Congress website “www.congress[.]gov” offline for ninety (90) minutes via DDoS attack.

In conclusion, Killnet is a rising threat organization with significant attack capabilities and an ever-growing catalog of newly compromised assets. Since the beginning, Killnet has utilized DDoS attacks in the majority of their campaigns, with some conducted by their elite “Legion” group. As tensions continue to grow from the conflict, CTIX analysts predict continued attacks from the Killnet organization against those who are allied with Ukraine or provide financial, military, or asylum to Ukrainian citizens.

Trending IOCs

The following technical indicators of compromise (IOCs) are associated with monitored threat groups and/or campaigns of interest within the past sixty (60) days. IOCs can be utilized by organizations to detect security incidents more quickly and easily, as indicators may not have otherwise been flagged as suspicious or malicious.

Indicator	Type	Attribution
5.2.69.50	IP Address	Killnet
92.255.85.237	IP Address	Killnet
92.255.85.135	IP Address	Killnet
173.212.250.114	IP Address	Killnet
144.217.86.109	IP Address	Killnet
156.146.34.193	IP Address	Killnet
162.247.74.200	IP Address	Killnet
164.92.218.139	IP Address	Killnet
171.25.193.25	IP Address	Killnet
171.25.193.78	IP Address	Killnet
185.100.87.133	IP Address	Killnet
185.100.87.202	IP Address	Killnet
185.129.61.9	IP Address	Killnet
185.220.100.241	IP Address	Killnet
185.220.100.242	IP Address	Killnet
185.220.100.243	IP Address	Killnet
185.220.100.248	IP Address	Killnet
185.220.100.250	IP Address	Killnet
185.220.100.252	IP Address	Killnet
185.220.100.255	IP Address	Killnet
185.220.101.15	IP Address	Killnet
185.220.101.35	IP Address	Killnet
185.220.102.242	IP Address	Killnet
185.220.102.243	IP Address	Killnet
185.220.102.253	IP Address	Killnet
185.56.80.65	IP Address	Killnet
185.67.82.114	IP Address	Killnet
185.83.214.69	IP Address	Killnet
195.206.105.217	IP Address	Killnet
199.249.230.87	IP Address	Killnet
205.185.115.33	IP Address	Killnet
209.141.57.178	IP Address	Killnet
209.141.58.146	IP Address	Killnet
23.129.64.130	IP Address	Killnet
23.129.64.131	IP Address	Killnet
23.129.64.132	IP Address	Killnet
23.129.64.133	IP Address	Killnet

23.129.64.134	IP Address	Killnet
23.129.64.137	IP Address	Killnet
23.129.64.139	IP Address	Killnet
23.129.64.142	IP Address	Killnet
23.129.64.147	IP Address	Killnet
23.129.64.148	IP Address	Killnet
23.129.64.149	IP Address	Killnet
23.129.64.210	IP Address	Killnet
23.129.64.212	IP Address	Killnet
23.129.64.213	IP Address	Killnet
23.129.64.216	IP Address	Killnet
23.129.64.217	IP Address	Killnet
23.129.64.218	IP Address	Killnet
23.129.64.219	IP Address	Killnet
45.153.160.132	IP Address	Killnet
45.153.160.139	IP Address	Killnet
45.154.255.138	IP Address	Killnet
45.154.255.139	IP Address	Killnet
45.227.72.50	IP Address	Killnet
72.167.47.69	IP Address	Killnet
81.17.18.58	IP Address	Killnet
81.17.18.62	IP Address	Killnet
91.132.147.168	IP Address	Killnet