Monthly Review

Cybersecurity news from around the world

GENERAL CYBERSECURITY NEWS 2

ARTICLES

Urge for regulation of commercial spyware 4

Two years of cyber war 7

KEY TAKEAWAYS 10

ARTICLE

Two years of cyber war

Read article →

SECTRA

General cybersecurity news

1 Major botnet disrupted by authorities

At the turn of January and February, the Federal Bureau of Investigation (FBI) announced that it had succeeded in disrupting the Chinese threat actor Volt Typhoon and the botnet it controls. This was made possible after the FBI gained access to the botnet's servers and managed to send orders to infected devices, mainly routers, to uninstall the malware and leave the botnet. Botnets are networks of hundred of thousands of devices that can be managed simultaneously. At present, botnets mostly contain various IoT (Internet of Things) devices, as it is often harder to notice that they end up as a part of a botnet network. The most typical use of a botnet is to exploit it in a denial-of-service attack. Volt Typhoon is a Chinese state actor known especially for cyber espionage targeting critical U.S. infrastructure. Its trademark has been exploiting security vulnerabilities in routers, VPNs and, more generally, outdated and unupdated devices. According to a January report by security firm Security Scorecard, Volt Typhoon managed to infect up to 30% of certain types of Cisco routers in about a month after discovering a suitable vulnerability. The best way to protect your devices from ending up in a botnet is to maintain up-to-date security updates, monitor network traffic for hijacking, and ensure proper protection against various cybersecurity vulnerabilities.

2 Deepfakes cause worry in the US preparing for elections

U.S. security officials, including the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), have expressed concerns about potential outside interference in the upcoming presidential election, particularly through the use of deepfakes. Deepfakes, produced using AI-based machine learning, can spread mis- and disinformation, influencing election outcomes. Incidents in January during the Democratic primaries saw fake phone calls used to manipulate voting in the state of New Hampshire. Concerns have been raised about foreign interference, especially from China due to their advanced AI capabilities, other players, such as Russia, cannot be ignored based on their past actions. This issue isn't limited to US elections, as Slovakia's recent elections witnessed the impact of deepfakes as well. To combat potential interference, fact-checking, source criticism, and good media literacy are essential.

3 Sweden accelerates digital transformation towards 2030

According to the 2023 annual review by the Swedish Military Intelligence and Security Service (MUST), they aim to achieve a relative information advantage against threat actors Russia and China by 2030 through extensive digital transformation. The importance of digital advancements in intelligence has been demonstrated in the ongoing war in Ukraine.

MUST emphasizes that organizations unable to utilize data assets and develop digital operations will be at a comparative disadvantage. To achieve this goal, Sweden needs to invest in its intelligence, security services, and military capabilities, focusing on digital transformation, innovation, and data protection.

The report highlights the need for Sweden to focus on digital advancements and strengthen its intelligence infrastructure to mitigate threats and maintain a competitive edge in a rapidly evolving world.

ARTICLE

Urge for regulation of commercial spyware

A couple of weeks ago, several countries and companies, including Microsoft, Google and Meta, as well as numerous organizations, signed a joint agreement led by France and Britain to address the threat posed by commercial spyware.

The most well-known spyware includes Predator, developed by Cytrox, and Pegasus, developed by NSO Group. Both have been used, for example, to track opposition politicians, human rights activists and journalists in several countries. Their feature is that delivering malware doesn´t require an error from the target, but they can be installed discreetly on the device as a so-called zero-click. This has guaranteed access to all the functions of the phone, including files, camera and microphone. Spyware has been seen as a threat not only to the privacy of the people it targets, but also to human rights and democracy more broadly.

Instead of a total ban on spyware, the agreement now signed aims to tackle its unethical use and distribution. The agreement states that the uncontrolled distribution of spyware contributes to unintended escalation in cyberspace. At the same time, they pose risks to cyber stability, human rights, national security and digital security. Four key terms are used to change this situation: accountability, precision, oversight and transparency. This means, among other things, that operations should be carried out responsibly on the basis of existing international and national legislation, and that operations should be restricted and supervised. At the same time, business operations should be responsible, interactive and comply with good business practices for both service providers and users. →

Regulating commercial spyware and its implications

Although the agreement and its objectives are appropriate in themselves and lay the foundation for international rules in the cyber world, the discussion and thus regulation seem to be overdue, as in the cyber dimension in general. Spyware has been talked about for years, and the first version of Pegasus, for example, was released back in 2011. Over time, commercial spyware has become an ecosystem of its own, with several companies offering the service. Attempts have been made to restrict their operations before, and NSO Group, which developed the Pegasus spyware, has been placed on the US sanctions list.

"It is abundantly clear that countries are developing their own capacities and are interested in these capabilities."

Attempts to control the spread of spyware developed by commercial operators and ensure its ethical use seem hypocritical. It is abundantly clear that countries are developing their own capacities and are interested in these capabilities. In addition, the effectiveness of the agreement is undermined by the absence of Israel and Israeli companies from the table, because the country has been a forerunner in development and use of spyware. Cyber espionage can also be carried out through other means than those mentioned. For example, Chinese Huawei has been suspected of possible backdoors to its network infrastructure. →

The process of creating rules for commercial spyware will continue in 2025, when the signatories will meet again to discuss the topic at a follow-up conference. Nevertheless, it is certain that the threat posed by commercial spyware will not diminish in the future. More players can be predicted to enter the market, because authoritarian states in particular will continue to be interested in these services. Neither will the cybercriminals follow these kinds of agreements, and many state actors will use also their services. ■

ARTICLE

Two years of cyber war

The cyber environment as one of the fields of warfare is the phenomenon of modern conflict concretized by the war in Ukraine, which previously could only be discussed in the form of theories or guesses.

Cyber struggle between states, or even cyber war, is nothing new per se, but the war in Ukraine is the first in which the fighting in the cyber environment coincides with a physical conflict and a state of war between the parties. Particular interest in cyber operations is how warring parties have tried, succeeded and failed to leverage their cyber capabilities to achieve broader strategic objectives and combine them with conventional warfare and broader hybrid warfare.

Before the start of the conflict there were many estimates of how and where cyber operations would play a role. In particular, there was a lot of talk about Russia's superior capabilities. The expectation seemed to be that Russia, with its advantage, would bring Ukraine to its knees with its cyber power by crippling critical infrastructure nodes and disrupting the communications network. The war began with a massive wave of cyberattacks, but contrary to what had been anticipated, these failed to achieve a significant, or at least a long-lasting, impact on Ukraine's ability to wage physical war. After the first few months, there was widespread speculation as to why this had not happened. Was it Russia's failure, Ukraine's surprising ability to protect itself and recover from attacks, or something else entirely? →

The evolving role of cyber operations

A lot of reasons were found. The most significant of these have been considered to be the support provided by foreign countries, especially the United States, and the relocation of critical data centers outside missile range or outside the country. In the first year of the war, many people believed that the most powerful weapons were being saved for later use and that's why there hadn't been any major cyberattacks yet. After all, cyber weapons are disposable in the sense that once a weapon has been fired, it is much easier to protect against it in the future when its operation method (i.e. typically very advanced malware) is known. For this reason, it was thought that Russia, which supposedly possessed these weapons, had not yet found it necessary or useful enough to use them. The assumption was that weapons would be kept in reserve until the damage they could achieve was maximum. This moment was thought to be the first winter of the war, when Ukraine's supply security would be stretched to the limit, and the war that has been going on for a long time has exhausted energy and raw material reserves. However, winter came and went without a massive impact cyberattacks from Russia. Of course, smaller-scale cyberattacks continued to occur on both sides, but neither side was able to achieve a devastating or long-lasting impact.

Over time, people started to realize that cyber weapons created before the war were actually being used or were being detected and prevented by protective measures in place. As a result, the talk turned from successes or failures in carrying out operations to the idea of whether cyber operations could after all be used effectively in war. Although it seems clear from current understanding that the conflict in Ukraine, or probably any other ongoing or near-future war, will not be resolved in cyberspace, what is happening on this battlefield should not be downplayed when looking at the conflict as a whole. Cyber operations have played a significant role, for example, in intelligence gathering. Ukraine, in particular, has also made effective use of cyberattacks to make the conflict tangible for the Russian people. The role of cyber activities is also often extremely difficult to assess, as information about all operations or their effectiveness is not shared publicly. →

This is particularly true in intelligence-related projects, where cyber activities are currently thought to be most useful. When assessing the significance of cyber operations, it should not be forgotten that although no lasting damage has been achieved, both sides have had significant, although temporary, effects with their cyberattacks throughout the conflict. Ukraine's strikes also show both development and growth when looking at operations in recent months.

It's hard to say how much cyber operations were relied on before the conflict began. Russia may have overestimated their capabilities. The evidence suggests that Ukraine, with US help, successfully removed malware from its systems just weeks before the war.

Thus, a cyber weapon is functional, but its role was previously misunderstood. Its primary purpose, in the light of current knowledge, is not to destroy or paralyze, but to obtain information, prepare operations, consume the resources of the opposing side and make war felt throughout society. Both sides have succeeded in this. ■

Key takeaways

1. There is concern in the United States about disinformation about the upcoming elections, in particular about the impact of deepfakes on electoral behavior.

2. Unupdated or poorly protected devices can end up as part of a botnet. As a result, devices can end up as part of criminal activities such as denial-of-service attacks.

3. Sweden focuses on digital transformation to enhance its information advantage, according to a 2023 report.

4. An international will has emerged to establish the rules of the game for the use of commercial spyware.

5. The Ukraine conflict demonstrates the convergence of physical fighting and cyber warfare, revealing cyber weapons' main purpose as intelligence gathering and resource consumption without causing lasting damage.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

SECTRA