ESET INDUSTRY REPORT ON GOVERNMENT:

Targeted but not alone

CYBERSECURITY
EXPERTS ON YOUR SIDE

TABLE OF CONTENTS

1

APT GROUPS, CYBERCRIMINALS AND THE NEED FOR RESILIENT IT SECURITY FOR GOVERNMENT

INTRODUCTION

Despite the pitfalls in making predictions during a pandemic, we can be confident cyber-risks for government bodies will continue to grow, evolve, and require even greater focus and resources to mitigate. Government, like industry, is facing the fact that its productivity tools are being turned against its interests and its ability to protect and provide essential services, ensure economic stability, and even maintain cultural and societal cohesion.

Andy Garth
Government Affairs Lead

The path to "digital by default"

Of course, these heightened risks come at a time when government bodies and businesses are still navigating a course through the coronavirus pandemic, adding to what is already a complex operating environment for those responsible for IT infrastructure and security. While there are differences between the functions of different government bodies, the overall trend is that the attack surface is expanding. This is reinforced by the fact that government bodies are edging toward digital services that are so straightforward and convenient that all those who can use them will choose to do so.

These elements include further rollout of citizen-facing systems, moving to the cloud, increasing use of third-party suppliers and service providers, and rapid onboarding of many users due to home or hybrid work becoming part of the new operating model. Being implemented at pace, these elements add to the challenge of maintaining system resilience in the face of sustained and evolving threats from advanced persistent threat (APT) groups and cybercriminals. Throw in keeping an eye on the regulatory scene and operating within tight budgets, and there is certainly plenty to keep a CISO awake at night.

COVID-19

Coronavirus lockdowns and the subsequent surge of employees accessing both company and institutional data, as well as IT infrastructure, from home did little to dampen the interests of cybercriminal gangs and nation-state actors. Indeed, both groups exploited this tumultuous period to pursue their respective goals, often with increased intensity and persistence. For example, during the pandemic, RDP attack attempts in particular *increased* by 768% between Q1 and Q4 2020.

Other threats detected by ESET specifically leveraging COVID-19 as a topic of interest include the mimicking of government services; for example, a "Canadian Government" *contact tracing app*. Amid COVID-19 lockdowns, steady servings of *phishing with "official Colombian Government" email correspondence* and watering hole attacks on Southeast Asian governments *courtesy of OceanLotus*, among others, have seen the interface between government and its citizens under assault.

With pressure already on governments to mitigate health impacts from COVID-19, reports abound of cyberattacks affecting service delivery to citizens, data theft, or the compromise of strategic national infrastructure. Some of the most prominent of late include the *SolarWinds Orion hack*, the *Microsoft Exchange exploitation*, attacks on the *Centreon* IT infrastructure monitoring tool, deliberate targeting of healthcare systems in France and Germany, and increased attacks on schools, universities, and education IT platforms.

Looking at the data and overall trends, we expect APT groups and cybercriminals to continue to hone their tactics that capitalize on COVID-19-related concerns and an increase in the targeting of widely used applications. In early 2020, for example, the XDSpy APT group operators *crafted an email* purportedly from the Belarussian authorities that claimed to confirm the first cases of coronavirus in Belarus. However, not only was this a work of disinformation making its rounds on social media networks, but it also contained a link to a piece of malware.

Cyberespionage

The traditional nemeses of government bodies are believed to be state actors looking to steal sensitive data and increasingly seeking to embarrass, undermine, and disrupt in order to secure their political and economic objectives. Such contests between states regularly happen in the gray zone where they can engage each other under the premise of plausible deniability. Now within this traditional cyber-sport, we see in the economic sphere—a constant high-priority target—a significant uptick in pursuit of purloining intellectual property, including the *targeting of vaccine developers* and their supply chains. These activities brush up against, if not outright crash into, governments' ability to protect and provide services to citizens.

With the attackers seeking to steal data or influence events in the real world, the gamut of the public sector, from national to local, should now adapt its posture to factor in targeting by these state actors—not merely as targets of criminal groups or lone hackers. State actor activity is increasing, yet there will be some bodies who think they would be unlikely targets of these actors. Unfortunately, all too often—given interconnectivity—state vs. state contests in one area of the globe have inadvertently affected systems in countries and organizations unrelated to those contexts. So, becoming collateral damage in these growing battles in cyberspace is a genuine risk.

One example of an APT group that at times seems to act rather boldly, making no efforts to hide, is *Gamaredon*, whose modus operandi includes the use of template injectors targeting ever-popular applications like Microsoft Word and Excel, and mass-mailing macros in the near ubiquitous Microsoft Outlook to target, for example, individuals at various Ukrainian institutions. By homing in on legitimate tools used across government and businesses, Gamaredon is very effective at fingerprinting a machine, understanding what sensitive data is available, and then spreading throughout the network. We have recently documented the group's move to custom-developed malware.

With impressive tools that include fileless malware, such as a custom open-source PowerShell loader to thwart detection, or its *LightNeuron* malware tailored to wreak havoc on the now all-too-preyed-upon Microsoft Exchange servers, the Turla APT group is mainly interested in high-profile targets such as government bodies and defense companies. Not to rest on its laurels, Turla created a new version of *Crutch*, which we documented in Q4 2020, that monitors external drives and abuses cloud storage for command and control communications.

Ransomware: Innovation and steady pressure

In the strata where state-sponsored actors blend with APT groups more criminal in nature, we can view the shift toward targeted ransomware attacks as an indicator of growing concern to government bodies and the businesses that they engage with. In addition, the phenomenon of several criminal groups working in cooperation to gain entry, steal or encrypt data, arrange payment, and launder the proceeds stands as a clear worry.

ESET's October 2020 collaboration with Microsoft, NTT Ltd, and multiple law enforcement agencies to disrupt Trickbot botnets revealed complex activity that included operators moving from attempting to steal money from bank accounts to compromising whole organizations with Trickbot and then using it to execute Ryuk to demand a ransom to unlock the affected systems. Interestingly, as Trickbot activity tapered off, *rising detections in ESET telemetry* for the Emotet botnet signaled a ramping up of activities, including even downloading Trickbot.

The emerging connection ultimately saw another botnet disruption in January 2021, against one of the longest-lived and most pervasive malware threats, *Emotet*. Led by Europol, this large-scale disruption operation included a number of national law enforcement agencies across Europe and North America.

With stakes this high, security staff tasked with defending service provision and internal processes are also sandwiched between staying vigilant for state actors and constantly facing maturing tactics, techniques, and procedures from APT groups. Furthermore, the emergence of this organized criminal industry with clear product and service offerings demonstrates innovation and drive among attackers. These groups have moved beyond assessing potential victims and obtaining the largest payout to maximizing the sale of data on now well-established criminal marketplace platforms.

Furthermore, via persistence, these groups can often spend weeks or months inside targeted systems conducting reconnaissance, harvesting data, and *eventually deploying ransomware*. While for some it will be a means to top up their funding, for others, the objective is more about undermining the host government and the services it oversees. Despite *many governments openly stating they do not pay ransoms*, they can still be victimized—including via "spray and pray" techniques – which can be distracting and resource intensive to deal with and, if successful, equally devastating.

Supply-chain attacks scaling rapidly

Supply-chain disruption, whether by accident or by design, can be traced to antiquity, as can its protection or improved resilience. However, digitization and the collaborative benefits derived from third-party providers have in turn *increased the risk of supply-chain attacks*.

The *DiskCoder.C* (aka NotPetya) attack in 2017 demonstrated this well, when the regionally popular M.E.Doc accounting software used by a number of businesses and their partners along a supply chain was weaponized to disrupt users' businesses. However, collateral damage—anticipated or not—impacted major global businesses, ironically many involved in logistics serving the world's physical supply chains. Fast-forward three years, and instead of weaponized accounting software, we've encountered a very large persistence campaign in the *SolarWinds Orion hack*. The attack impacted thousands of users across that platform and opened up the potential for widespread criminal and APT group activity across the board.

ESET researchers have uncovered several other supply-chain attacks over the past several months, from the *Lazarus group* using hacked security add-ons, to *Operation Stealthy Trident* attacking region-specific chat software for businesses, *Operation SignSight*, used to compromise a government certificate authority, to *Operation NightScout*, a hacked Android emulator.

Home, the new normal workplace

Home and hybrid working have significantly increased the risks for all employers and hence government bodies. It is clear that these arrangements will endure and continue to be a source of concern as some form of ongoing hybrid working becomes part of the operating model post-COVID-19. From a system security point of view, the home environment can feel more like the Wild West with "homesteads" and "outposts" more exposed to cyberattacks from a seemingly ever-growing crop of increasingly sophisticated cyberbandits looking to rustle up some action.

It is estimated that *23% of cybersecurity breaches are due to human error*. Attackers often take advantage of natural instincts to click (in milliseconds) on links masquerading as legitimate. However, some of the largest breaches have been through the actions of experienced IT professionals— who should have known better—including via connecting BYO devices, misconfiguring cloud systems, and other poor practices. Of course, increased staff training and strengthening processes are essential to embed the required security behaviors as instinctive.

And while a lot of attention is paid to hacker attacks, in its *2020 Cost of Insider Threats: Global Report*, Ponemon Institute revealed that the number of reported incidents caused by insiders increased by 47%, from 3,200 in 2018 to 4,716 in 2020. Many of these breaches are due to human error, but some are insider attacks by *disgruntled employees*. This can include data theft, physical damage, and deletion of accounts—for revenge, personal profit, or to further the interests of a new employer or even a state actor. Such attacks, particularly by those with administrator privileges, are harder to detect without an endpoint detection and response tool or other advanced detection solutions manned by expert staff.

Targeted but not alone

In the current dynamic security environment, it is more important than ever not to overestimate your cybersecurity capability. Cyber-risk is increasing, not decreasing. Regular reviews, testing, and *attack scenario exercises* are increasingly essential to help you fend off attacks and quickly contain incidents. Due to the skills and tools available to state-backed actors, risks born of being targeted or from collateral damage now require complex multi-layered defenses, active monitoring, up-to-date *threat intelligence*, and an ever more educated security team.

Expanding your understanding of the ever-evolving threats will help you not only to better protect your own systems but also to better inform your stakeholders, businesses, and citizens who look to government bodies for guidance. In a year of much disruption and sadness, one of the positive trends in cybersecurity, as much as in the fight against coronavirus, is the emergence and importance of a strong partnership between government and the private sector to tackle these challenges. ESET welcomes this and looks forward to working with its government partners to better secure a safer digital world.

2

APT ATTACKS IN EUROPE: A GROWING MENACE TO GOVERNMENT

Do the past half year's attention-grabbing attacks conducted by APT groups signal business as usual, or an emerging trend in supply-chain attacks?

Robert Lipovský
Senior Malware Researcher

In the past six months, a rash of notable advanced persistent threat (APT) attacks have been revealed, targeting countries across the European continent, from France to Eastern Europe and the Balkans, and across verticals, from government and military entities to private companies.

An example of APT activity discovered by ESET is a new version of Crutch, a previously undocumented backdoor and document stealer belonging to the infamous Turla APT group. ESET researchers saw Crutch in the network of a ministry of foreign affairs in a European Union country. Another discovery was activity by *Gamaredon*, an adversary group known for its relentless targeting of governmental organizations in Ukraine – which *updated its malware arsenal* through 2020.

In the following text, we'll take a closer look at two other examples: *XDSpy*, an APT group that managed to stay under the radar for nine years, and Sandworm, which is one of the most dangerous APT groups in operation.

We'll also discuss the role supply-chain attacks play in the arsenals of various threat actors, a subject that has been grabbing even more attention than usual since the SolarWinds hack made international headlines.

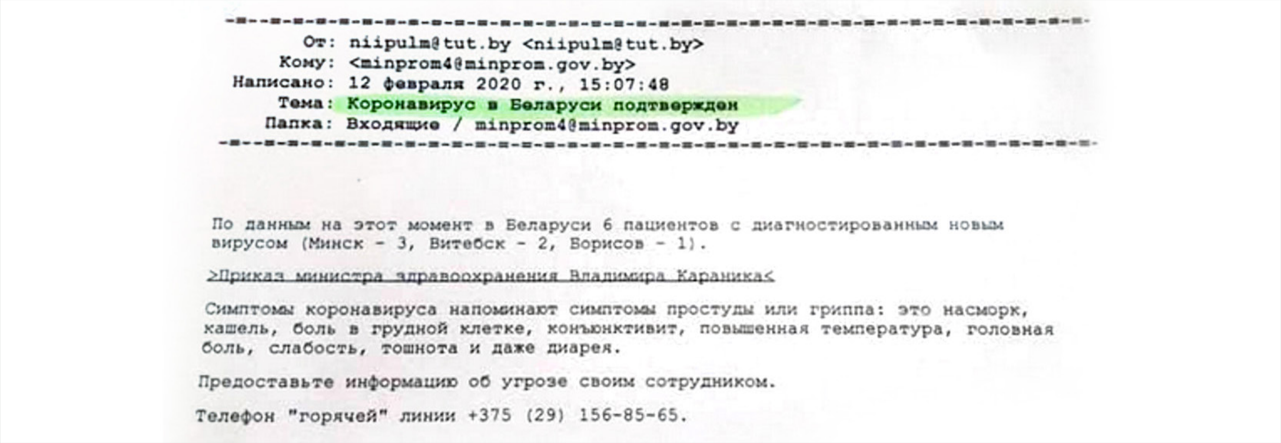
XDSpy – Stealing government secrets since 2011

Probably the most interesting characteristic of the XDSpy APT group is that it went largely unnoticed for nine years. This espionage group has been active since 2011, and its activities were undocumented until an *advisory* from the Belarusian CERT in February 2020.

Over the years, the group compromised many government entities, including militaries, Ministries of Foreign Affairs, and private companies in Eastern Europe and the Balkans. According to ESET telemetry, the targets of XDSpy were located in Belarus, Moldova, Russia, Serbia and Ukraine.

Of particular interest are two instances where the XDSpy operators used the COVID-19 theme in their spearphishing campaigns. In February 2020, they spread the malware through an email stating that the first cases of COVID-19 had been discovered in Belarus, even though this was a few weeks before the first official cases in the country were actually registered. The following photograph of the malicious email circulated on social networks as part of an unexpected disinformation campaign.

Then, in September 2020, the operators used the official Russian government COVID-19 website rospotrebnadzor.ru as a decoy to download XDDown, the main malware component responsible for downloading additional plugins.



```
-=--=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
        От: niipulm@tut.by <niipulm@tut.by>
      Кому: <minprom4@minprom.gov.by>
  Написано: 12 февраля 2020 г., 15:07:48
      Тема: Коронавирус в Беларуси подтвержден
     Папка: Входящие / minprom4@minprom.gov.by
-=--=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

По данным на этот момент в Беларуси 6 пациентов с диагностированным новым
вирусом (Минск - 3, Витебск - 2, Борисов - 1).

>Приказ министра здравоохранения Владимира Караника<

Симптомы коронавируса напоминают симптомы простуды или гриппа: это насморк,
кашель, боль в грудной клетке, конъюнктивит, повышенная температура, головная
боль, слабость, тошнота и даже диарея.

Предоставьте информацию об угрозе своим сотрудником.

Телефон "горячей" линии +375 (29) 156-85-65.
```

In terms of functionality and architecture, XDSpy uses a typical cyberespionage toolset consisting of a main downloader module that downloads additional plugins to carry out the desired actions. During our research, we discovered plugins used for exfiltrating files from the main C: drive or from external drives, taking screenshots, and extracting saved passwords from various applications, such as web browsers and email programs. One of the plugins, called XDLoc, is used to gather nearby SSIDs (Wi-Fi access point names), most likely to geo-locate victimized machines.

XDSpy operators use spearphishing emails in order to compromise their targets. The emails display a slight variance, as some contain an attachment, while others contain a link to a malicious file. The first layer of the malicious file or attachment is generally a ZIP or RAR archive. At the end of June 2020, the operators stepped up their game by using a vulnerability in Internet Explorer, CVE-2020-0968.

Exaramel backdoor in France: Another Sandworm supply-chain attack?

When it comes to the notorious Sandworm APT group, certainly, the most significant news in the past six months was the US Department of Justice *indictment* of six Russian GRU officers for their alleged roles in the group's many attacks.

Aside from the geopolitical aspect, defenders should be aware that, even though Sandworm's most infamous attacks were dated between 2015 (the *first Ukrainian power grid attacks*) and 2018 (*Olympic Destroyer*), this dangerous group is still very much active in 2021.

In February 2021, France's national information security agency ANSSI released a *report* revealing an intrusion campaign targeting the Centreon IT monitoring software, which resulted in the breach of a number of French organizations. The campaign lasted from 2017 until 2020 and affected mostly IT providers, especially web hosting providers. Two backdoors were discovered on compromised systems: the P.A.S. webshell and (much more interestingly) the *Exaramel* backdoor.

Exaramel is the work of Sandworm (more specifically, a subgroup that ESET tracks as TeleBots) and was the piece of evidence that allowed us to attribute the infamous *Industroyer* to the same APT group, based on code similarities.

With the recent SolarWinds hack in mind, and the fact that Sandworm is known for conducting supply-chain attacks in the past—remember the *M.E.Doc compromise* leading to the NotPetya outbreak?—the cybersecurity industry was immediately curious about details of the Centreon compromise.

According to *Centreon*, the compromise was not the result of a supply-chain attack. Instead, the campaign exploited installations of out-of-date versions of its IT monitoring software, not the company itself.

The fact that this was not a supply-chain attack is a positive finding, as finding otherwise would indicate a serious compromise with potentially far-reaching consequences. However, another fact still remains true: Organizations have been using vulnerable versions of Centreon IT monitoring software, and attackers have taken advantage of that in order to compromise them.

Future outlook

The past six months have shown that it's business as usual for APT groups—including highly sophisticated ones like Sandworm, less erudite (but still capable of staying under the radar and likely achieving their goals) ones like XDSpy, and everything in between.

Supply-chain attacks, while not all as earthshaking as the SolarWinds hack (or other occurrences, such as the recent Centreon case, that smell like supply-chain attacks but actually aren't), are becoming a major trend. In fact, in Q4 2020 alone, ESET uncovered likely as many supply-chain attacks as the whole sector saw annually just a few years back: the case of Lazarus abusing the *WIZVERA VeraPort* software used by government and banking websites in South Korea; *Operation StealthyTrident*, compromising the Able Desktop chat software used by several Mongolian government agencies; and *Operation SignSight*, compromising the distribution of signing software distributed by the Vietnamese government. More recently, in Q1 2021, ESET also uncovered *Operation NightScout*, a supply-chain attack targeting online gaming communities.

Considering how difficult it is to detect and prevent supply-chain attacks and how much APT actors and cybercriminals have to gain from them, the number of such attacks is only expected to grow in the near future, both in Europe and globally.

For that reason, keep in mind the following recommendations to reduce the risks that stem from vulnerable software supply chains:

- Know your software—keep an inventory of all open-source and proprietary off-the-shelf tools used by your organization.
- Keep an eye out for known vulnerabilities and apply patches as soon as they are available; indeed, attacks involving tainted updates should by no means discourage anybody from updating their software.
- Stay alert for breaches impacting third-party software vendors.
- Drop redundant or outdated systems, services and protocols.
- Assess your suppliers' risks by developing an understanding of their security processes.
- Set security requirements for your software suppliers.
- Request regular code audits and inquire about security checks, and change control procedures for code components.
- Inquire about penetration tests to identify potential hazards.
- Request access controls and two-factor authentication (2FA) to safeguard software development processes and build pipelines.
- Run security software with multiple layers of protection.

3

IT SECURITY AND GOVERNMENT: PARALLELS BETWEEN TARGETED INSTITUTIONS

To be CISO of a cybersecurity company is to be in a unique position. And, while there is inherent benefit in working with a board that intrinsically understands the technical aspects of security, cybersecurity companies are no less a target (indeed, they could be a prize) for cybercriminals. This second point, knowing we are a target, is where I believe our experience most strongly intersects with that of government organizations. This key point has remained constant over my 10 years as CISO at ESET and is a main driver in evolving our security posture to meet the ever-changing demands of the online environment.

Daniel Chromek

CISO/Section Lead

The reality of our status as a target also has strong relevance to our company's security culture, growth and business model. Governments face a similar challenge. They are clear targets, their adversaries will not be readily eliminated, and mitigation of the worst symptoms of the tactics and techniques found on the threatscape dictate everything from security policy and resource allocation to culture and strategic growth.

Questions about how to evolve can be answered both from the point of view of ESET and from that of the wider information security world. Since I am more intimately acquainted with ESET, it is far easier to address the "how" from that perspective. ESET is a company whose business has grown quite dramatically during my tenure. On the other hand, it is a close-knit community in which a lot of activities needed standardization and a proper governance framework in order to streamline internal processes, communication and the exchange of information.

In particular, standardization and governance at ESET supported us in shifting focus from protecting primarily consumer and SMB clients toward enabling significant growth in the enterprise segment. It is this pursuit that has added new pressure to document information security, comply with distinct directives and regulations, and enhance our capabilities to address enterprise customers' questions and reservations when implementing security solutions in their environments. Categorically , all governments are facing rapid demand to digitize services, improve internal processes—and to formalize both through improved governance. Similar to the ESET experience, the journey involved with formalization of processes (and culture) via governance reflects maturity and ambition to reach new markets; in the case of governments—improved growth, better service provision and national or local cohesion.

Implications of maturation

Of course, the challenges around governance were being faced well before we reached our current level of maturity—and with growth of the company, they have only become more complex. As such, deploying security controls in a complex IT environment requires more time and more resources than before. Therefore, our internal security section grew significantly and now consists of multiple teams focusing on various aspects of security.

Suffice to say that the internal security division needs to be very well prepared, as presentations to management can quickly morph into technical deep dives. The last time we had this type of deep dive, it was related to our vulnerability management tool's risk score parameter and the formula behind it so that management could understand whether it was suitable for reporting. This included a debate on how the presence of an exploit in malware kits can raise the risk score above traditional CVSS scores. Whether it was 12 years ago when I joined the co-founders in discussing our security policies or today, going deep remains a cultural phenomenon deeply rooted at ESET.

Of course, even before I took on the CISO role, we had many very skillful employees and needed to balance security and visibility against the "Big Brother" worries held by our colleagues. ESET's owners were privacy-aware and remain so. We also understood early on the possible impact on staff morale. So, we agreed to configure ESET culture early on as that of a positive security company, persuading everyone, including management, that using fear, uncertainty and doubt tactics simply do not work and could result in losing the respect of colleagues across the organization.

I raise this because all of us, you and I included, face a similar choice: balancing security and visibility with another component—trust. This need became painfully clear in 2020, *the year that gave us COVID-19* and that transported ESET, and likely all of us, to a security future few of us entirely expected. To succeed in security in the COVIDian era, a few basics have to be done right. These go beyond trust and include the practical aspects of security that need minding by CISOs in 2021. Please find mine below:

1. Keep basic principles running in work-from-home mode

"Getting back to basics" is always good advice in information security. It also applies to 2021, when we hopefully enter a post-COVID world. Patching, backups and endpoint protection are areas that are important regardless of where employees work, whether in the office or from home. Expansion and management of staff VPN accounts to provide more secure access to an organization's platforms, along with many other precautions, are here to stay. Considering a Zero Trust security approach or a "trust but verify" narrative might be helpful when addressing remote work specifics. Keep an eye on these and look to optimize.

2. Grow the organization in regulated areas

While I can only speak for ESET, we see accelerated growth in security-related regulations all over the world. This will likely increase exponentially with the already rapid digitization being accelerated by COVID. For example, the NIS Directive (and the *NIS2 Directive*) impacts both ESET as a cybersecurity provider and many of ESET's clients, especially those in regulated industries or those that provide direct services to government. So, it makes sense that we engage together to create shared approaches.

Just last year, amid rolling COVID lockdowns, ESET and its products entered new regulatory territory with the launch of our cloud services like ESET PROTECT Cloud. This brought its own complexities, with ESET again needing to comply with the NIS Directive and ESET's partners having to navigate local laws regulating the use of cloud-based security software. So, while having to comply with a single regulation like the NIS Directive may not be pleasant, it is still a more straightforward task than aligning with multiple regulations and standards required by government, industry and enterprise customers.

To face these challenges, a good approach is to establish an information security management system (e.g., ISO 27001) to manage your core information security processes and then systematically add the rest of the security controls you need to bring your organization up to speed with compliance. ISO 27001, as well as the Building Security In Maturity Model (BSIMM), can help organizations develop and maintain good documentation of their security management system and internal controls, which is a must to prove compliance.

3. Balance resources to support various business initiatives while preserving team sanity

I believe we struggle with this point as an industry. Likely, the main problem faced by any mature security program is its relationship with so many activities within the organization; simply, it is difficult to give priority to the truly important activities. Reporting and measurement add another level of complexity—we should track risks, audit findings and incidents; gather feedback and lessons learned; identify compliance gaps; etc., even though sometimes it feels like we are being asked to compare what is incomparable. This same challenge is certainly relevant for government organizations too as they strive to strike a balance between the security of internal mechanisms and external services with reporting—all of which needs to be both compliant and functioning practically.

But there are at least two ways to achieve equilibrium. The first is by way of business priority. If business can identify their priorities, then it is easy to shift internal security resources to them. If, however, business cannot identify their priorities (whether overall or compared with other business unit priorities), the key to finding a solution seems to be by asking the following questions: What is the risk? What is the risk if our security team cannot dedicate resources to support the business initiative? What is the risk that a particular audit's finding won't be closed? What is the risk of…you name it! Risk can be used as a single measure of determining the priority of competing activities.

4. Increase the maturity of your software development life cycle

In the enterprise world, it is quite common to have both internal and outsourced development teams that build, customize and maintain critical systems, products or services. A problem that can thus arise in the face of multiple security standards being used in the software development life cycle is the expectation of applying a waterfall model. However, with a strong push on rapid agile development and deployment ongoing in the industry, it is simply not viable to apply a waterfall approach to DevOps activities any longer.

ESET's approach is to define DevOps security activities, related to both development and operations, and to engage in patient discussion with development teams as to how to include these activities in their methodologies and work procedures. The goal: to identify what should be delivered by internal security experts, versus security champions within the diversity of development teams, and how to automate as much as possible.

5. Prepare and respond to the growing complexity of attacks

Looking at *Verizon's data breach reports* over the years clearly suggests that attacks are getting worse. We don't know what kind of vulnerabilities may be exploited next, what kind of tools attackers will use, or what their goals are. But what we can do is to prepare for them: both technically, via layered controls, and organizationally, with incident response team capability, skills and overall maturity.

The situation brought on by COVID-19 has been a good reminder of how quickly things can change. The accelerations COVID brought to ESET are likely similar to those experienced by other organizations. My chief takeaways from this experience would be:

- To put more focus on asset categorization and endpoint visibility as employees are working from home, outside of an organization's on-premises network.
- If leveraging cloud-based services, to prioritize proper configuration, access management and resource allocation, among other cloud security measures.

From our own experience, we've noticed a clear growth in attacks, especially Business Email Compromise (BEC), that demanded more of our attention than usual. We are lucky, as our endpoint portfolio includes a solid anti-malware engine, a cloud-managed sandboxing solution—*ESET Dynamic Threat Defense*—against emerging threats, and an endpoint detection and response solution—*ESET Enterprise Inspector*—that provides a ton of visibility into endpoints and boosts our incident response capabilities. Furthermore, we also have an easy-to-use Data Loss Prevention solution via our technology alliance with Safetica.

Targeted but diligent

Yes, we remain targeted, but having a solid foundation, including the components mentioned above and a deep focus on governance, enables us to focus on specific problems like forensic evidence, and gathering and reworking these findings into our own products. This is where our expertise in malware research most clearly intersects with product development. Using ESET Enterprise Inspector in combination with our core detection technologies, we can simultaneously protect the business and constantly evolve our systems, culture and processes to meet the challenges of the moment.

4

EMISSARYSOLDIER: MALICIOUS ACTIVITIES OF LUCKYMOUSE APT GROUP IN 2020

LuckyMouse has compromised government networks and private companies (telco, media and banks) in Central Asia and the Middle East

Matthieu Faou
Malware Researcher

LuckyMouse, also known as APT27 and Emissary Panda, is a cyberespionage group that is best known for its regular use of watering hole, or strategic web compromise, attacks. The group has breached not only multiple government networks in Central Asia and the Middle East, but also transnational organizations such as the International Civil Aviation Organization (ICAO).

In its latest analysis of LuckyMouse, ESET Research discovered a set of malicious activities that took place in 2020 and in which the operators mainly used the SysUpdate (aka Soldier) toolkit. ESET has named this set of activities EmissarySoldier.

In order to compromise victims, LuckyMouse typically uses watering holes, compromising websites likely to be visited by its intended targets. LuckyMouse operators also perform network scans to find vulnerable internet-facing servers run by their intended victims. While the group generally uses already known exploits to compromise unpatched servers, ESET saw LuckyMouse among the threat groups likely leveraging the Microsoft Exchange vulnerabilities while they were still zero days to conduct attacks on email servers.

Once LuckyMouse operators gain a foothold on a machine, they will deploy one of their custom post-compromise implants, SysUpdate or HyperBro. An interesting similarity among their toolkits is that they all employ DLL search order hijacking to thwart detection.

code execution vulnerabilities were found in this application. While ESET doesn't have proof that these exploits were used, we did observe LuckyMouse components being deployed through the internet information services (IIS) instance that was also serving Microsoft SharePoint.

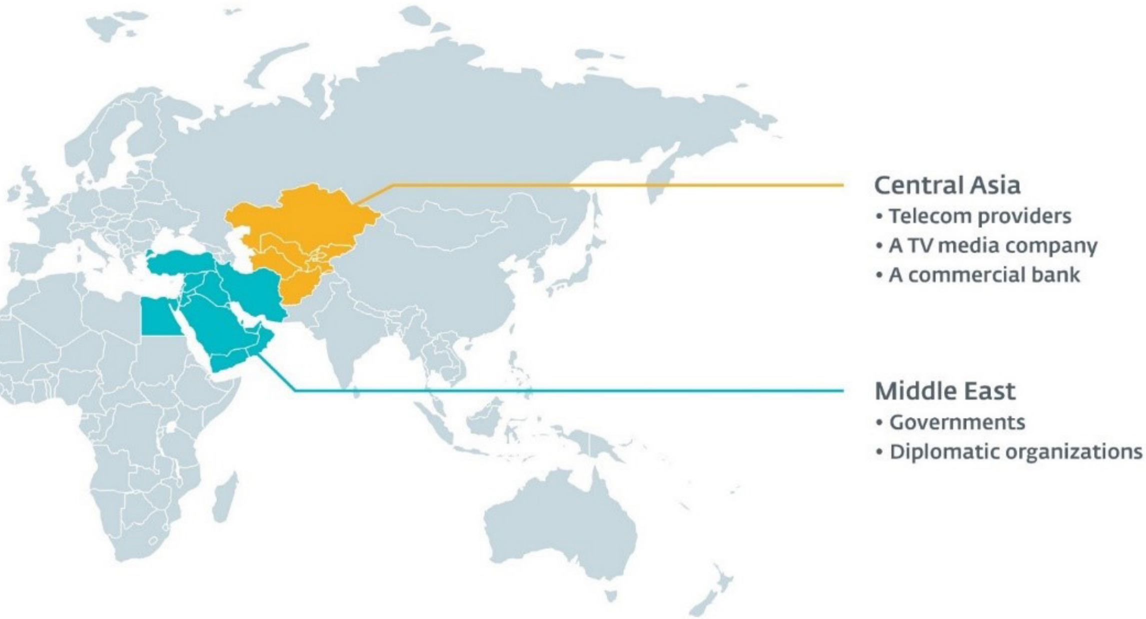


image: According to ESET telemetry, LuckyMouse targeted the following entities in 2020

The Middle East is currently a hotbed for many espionage groups, and LuckyMouse has been very active there as well. It is very common to find multiple threat actors on the same machine or at least in the same network. In this region, LuckyMouse predominately focuses on governmental entities. The operators are probably trying to obtain insights about the current geopolitical situation. On the contrary, most of their targets in Central Asia are private companies (telco, media and banks). This shows a strategic interest in the economic situation of the region.

LuckyMouse maintains a quite large network infrastructure with VPN nodes, staging nodes and command and control (C&C) nodes. During the EmissarySoldier campaign, ESET observed 16 different staging and C&C nodes.

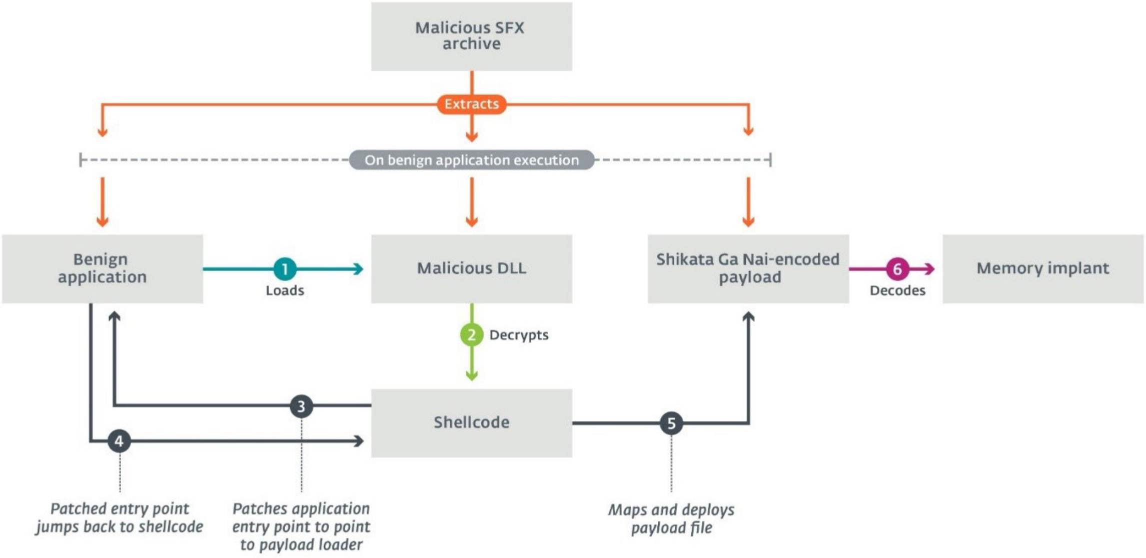
ESET researchers also noticed that some of the compromised machines were running Microsoft SharePoint, which was reachable from the internet. In 2019 and 2020, several remote

LuckyMouse has a specific way of installing its implants—using a so-called trident model—in its SysUpdate toolkit. The trident model features a legitimate application vulnerable to DLL hijacking, a custom DLL that loads the payload, and a raw Shikata Ga Nai-encoded binary payload.

Overview of the trident model

Typical of many financially motivated—but also espionage—threat actors, LuckyMouse employs offensive security tools. Thus, while the group mainly uses custom backdoors, ESET researchers have seen several other tools in some intrusions, including:

- JuicyPotato, a privilege escalation tool;
- Mimikatz, a tool to extract various Windows secrets, including passwords; and
- nbtscan, a NetBIOS scanner.


Malicious SFX archive
Extracts
On benign application execution
Benign application
1 Loads
Malicious DLL
Shikata Ga Nai-encoded payload
6 Decodes
Memory implant
2 Decrypts
Shellcode
3
4
5
Patched entry point jumps back to shellcode
Patches application entry point to point to payload loader
Maps and deploys payload file

The SysUpdate toolkit itself, which was the focus of this latest deep dive into LuckyMouse activity, is relatively new, with the first samples having been discovered in 2018. Since then, the toolkit has been through various development stages. In contrast with previous samples, those used in 2020 showed major improvements and added functionalities, including the implementation of multiple C&C communication protocols and small refactoring of already implemented features.

SysUpdate components are divided into a set of binaries, each with a specific operational purpose. In particular, the trident model components of SysUpdate consist of a benign application like GUP.exe, which acts as the initial loader for the next component, a DLL, which in turn acts as a loader for the next component, the Stage 1 payload itself. These three components are dropped to an arbitrary location on initial access to a compromised system, a pattern that seemed to be recurrent in the activity monitored across different victims located in different regions.

As the SysUpdate toolkit is highly modular, it gives its operators the flexibility to provide malicious capabilities on demand, as well as pull back and limit the exposure of malicious artifacts at will. For this very reason, ESET researchers did not retrieve any malicious modules, and they expect this to be a recurrent challenge in analyzing future operations that employ SysUpdate. The best way of tracking down such a slippery customer is by deploying an endpoint detection and response (EDR) solution that can identify suspicious events happening in a network. LuckyMouse was increasingly active throughout 2020, seemingly going through a retooling process in which various features were being incrementally integrated into the SysUpdate toolkit. This may be an indicator that the threat actors behind LuckyMouse are gradually shifting from using HyperBro to SysUpdate.

HyperBro is a much older toolkit that has caught significantly more attention from the threat intelligence community in recent years, with considerable evidence suggesting it has also been adopted by several APT groups. On the other hand, SysUpdate has not received much attention, with few public reports mentioning it—most likely, it has only been deployed in a relatively small number of operations.

Monitoring LuckyMouse and the tools used in its recent campaigns remains a priority. A reminder of why occurred just as ESET researchers were wrapping up this investigation, with the threat group leveraging ***vulnerabilities in Microsoft Exchange*** to attack email servers and install the SysUpdate toolkit. This point of intersection provides a strong case for governments and business alike to tighten up security on internet-facing servers, further collaborate on security strategy, and build capacity and maturity in the use of EDR tools.

5

REGULATORY RADAR: CRITICAL CUES FOR CYBERSECURITY POSTURE IN THE EU AND US

Society's reliance on technology, and the emergence of those who seek to misuse it, have led to increasing attempts by governments around the globe to regulate cyberspace. In doing so, governments are broadly attempting to deter bad actors, both state-sponsored and criminal, through powers to pursue and levy penalties; protect critical national infrastructure, personal information, security and defense assets; and build societal resilience by ensuring government bodies, businesses and other organizations recognize their responsibilities and are held accountable. In parallel, governments aim to educate citizens as to the scope of cybersecurity risks and needed mitigations.

Andy Garth

Government Affairs Lead

At a supranational level, the United Nations is trying to secure agreement on the application of international law to state activity and build on 11 norms of responsible behavior in cyberspace agreed in 2015. The European Union's 2018 GDPR regulation quickly became a reference point for countries seeking to strengthen privacy and security regulation. Both the EU and US (under the new Biden administration) are expected to set the tone for the increased regulation of cyberspace in the years ahead.

In the absence of a global standard or agreement, the regulatory picture is rather fragmented. Presently, regulation is predominately driven at the national, state and industry sector levels. This fact, combined with the pace of innovation and legislative complexities, has left most governments with palpable security challenges and many struggling to keep up.

Given the broad scope of cyberspace and differences in national approaches, for brevity, CISOs and policy makers should keep an eye on the following areas to identify critical cues for future compliance and security posture.

European Union: NIS2 Directive

In December 2020, the EU published the draft text of the NIS2 Directive, which significantly expands the number of entities and sectors required to take strengthened measures to enhance cybersecurity. The text is currently progressing through the legislative scrutiny process.

Once a final text is agreed, on member states will have 18 months to implement the directive. The impacts will be felt in the EU and beyond. **The proposed NIS2 Directive will:**

- Introduce more stringent supervisory measures;
- Impose stricter enforcement requirements, including harmonized sanctions regimes across member states;
- Establish information sharing and cooperation on cyber-crisis management at national and EU levels;
- Mandate the creation of national strategies that ensure the resilience of critical entities;
- Obligate the carrying out of national risk assessments; and
- Aim to strengthen the security of supply chains.

When adopted, the NIS2 Directive will apply alongside sector-specific legislation, such as the proposed "Directive on the Resilience of Critical Entities." This sector-specific directive aims to protect critical infrastructure and will complement the NIS2 Directive to the extent in which it will likely impose cybersecurity risk management and notification obligations of at least an equivalent effect to the obligations set out in the NIS2 Directive.

European Union: Cybersecurity Certification

The EU Cybersecurity Act of 2019, now in force, granted a permanent mandate to the EU Agency for Cybersecurity (ENISA), including the new key role of setting up and maintaining a cybersecurity certification framework. This framework will provide EU-wide certification schemes with a comprehensive set of rules, technical requirements, standards, and procedures, providing assurance to users based on the level of conformity with the agreed requirements.

Further, these certification schemes represent agreements at the EU level on the evaluation of the security properties of information and communications technology (ICT) products or services. Briefly, these will attest ICT products and services in terms of:

- categories of products and services covered;
- cybersecurity requirements;
- the type of evaluation; and
- the intended level of assurance.

ENISA and the European Commission will be assisted and advised by:

- European Cybersecurity Certification Group (ECCG);
- the Stakeholder Cybersecurity Certification Group (SCCG); and
- European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC).

In particular, the ECCC is expected to become the main instrument for investing in cybersecurity research, high tech and innovation. This overall mission will feed into the following objectives:

1. Carry out procurement of products and solutions.
2. Provide financial support and technical assistance to start-ups and SMEs.
3. Support research and innovation based on a comprehensive research agenda.
4. Drive high cybersecurity standards, especially in the field of skills development.
5. Facilitate cooperation between civil and defense spheres with regard to dual technologies (in relation to the European Defence Fund).

Tony Anscombe
Chief Security Evangelist

US privacy regulations and evolving cybersecurity laws

Following the EU's enactment of GDPR in 2018, implementation of data privacy regulations also began to gain pace at the state government level in the United States. Legislators in California passed the California Consumer Privacy Act in 2018 (CCPA) and implemented it in 2020. At the end of 2020, California's Proposition 24 was passed, meaning the California Privacy Rights Act (CPRA) will become effective in 2023. The CPRA makes significant additions to the CCPA—which itself could be seen as falling short of GDPR in some areas, although in others it went further. These include:

- the concept of household data in addition to merely individual data as emphasized in the GDPR;
- extending protection to Californian residents even when outside the state for temporary or transitory purposes;
- the right to opt out of the sale of personal data to third parties. Companies must include a "Do Not Sell My Personal Information" link on website home pages. While similar protections exist under the GDPR, they are less clear—a data subject needs to opt out of marketing purposes and additionally withdraw consent for processing activities.

With broad agreement on the need for federal consumer privacy legislation realized in the Consumer Online Privacy Rights Act (COPRA) in April 2020 and the Biden administration's apparent recognition of the need for federal privacy legislation, we will likely see a host of initiatives. Indeed, Vice President Kamala Harris has a strong record in privacy enforcement, as witnessed by the amended and strengthened California Online Privacy Protection Act (CalOPPA) during Harris's time as California's state attorney general. Also, several Obama-era staffers who contributed to the consumer bill are back in the driving seat.

As the pandemic continues, there will likely be considerable focus on healthcare providers and agencies that have been party to contact tracing, testing and vaccination. Currently, some of the processes for collection of personal data may not be as scrutinized due to urgency and medical need. It should be expected, however, that this latitude will likely be removed and the cybersecurity requirements for such data will be strengthened and enforced.

This is also true globally, where the internet creates an environment that breaks down international barriers, given that everything is accessible in the same cloud. Privacy legislation is not a set and done process; it's an evolving process that is likely to require continual modification, especially when considering new technologies such as artificial intelligence, the Internet of Things and other advancements in technology. There is a need for standardization and harmonization within and among states, countries, and continents across the globe. All consumers should be awarded the same data privacy rights by companies and organizations regardless of their location. Privacy legislation is undoubtedly a topic that will remain a priority for legislators.

Cybersecurity laws in the US

While there are all-encompassing cybersecurity laws in the US, typically legislation is dependent on the sector of a business or organization, although some legislation aimed at specific technologies crosses the boundaries of multiple industry sectors.

Some of the leading sector-specific US legislation related to cybersecurity includes:

- Health Insurance Portability and Accountability Act (HIPPA);
- Gramm-Leach-Bliley Act;
- Dodd-Frank Act; and
- IoT Cybersecurity Improvement Act.

- Consumer Privacy Protection Act 2017—requires companies to secure personal information and provide notifications on data breaches.
- Cybersecurity Information Sharing Act (CISA)—allows sharing of internet traffic between gov't and tech companies for cybersecurity threat reasons.
- Federal Information Security Management Act (FISMA)—requires government agencies to have policies, standards and guidelines on information security.

An example of sector-specific legislation is the HIPPA, which requires healthcare organizations to protect personally identifiable information from fraud and theft, and to address limitation in healthcare insurance coverage. In the financial industry, organizations are required to comply with the Gramm-Leach-Bliley Act and the Dodd-Frank Act, which stipulates there must be policy in place to protect information from security threats and issues with data integrity.

In fact, under the Dodd-Frank Act, the Consumer Financial Protection Bureau has authority to socialize potential new rules. Accordingly, in autumn of 2020, the bureau issued an Advance Notice of Proposed Rulemaking which will likely result in changes in the near future to the methods of consumer-authorized access to data and the level of data security required under the law.

IoT

Finally, the IoT Cybersecurity Improvement Act of 2020, which applies across sectors, requires the National Institute of Standards and Technology (NIST) to publish standards and guidelines for federal agencies on the appropriate use of IoT devices in government systems.

This piece of IoT legislation consists of a stepped timeline that requires agencies to:

- agree on how to address and disclose vulnerabilities of devices in use;
- set minimum information security requirements for managing cybersecurity risks; and
- review and revise guidelines and standards every five years.

The final component takes effect in December 2022 and will prohibit use of IoT devices that do not comply with the NIST standards and guidelines.

6

ENDPOINT DETECTION AND RESPONSE: A COUNTERBALANCE TO PERSISTENT THREATS

Large organizations and government institutions, such as ministries of foreign affairs, embassies and other diplomatic representatives, are prime targets for espionage operations. Threat actors target these institutions in various ways to steal sensitive information. Stealth is an essential part of these malicious campaigns because remaining unseen and undetected in a target network for as long as possible is key for success.

Endpoint detection and response (EDR) technology can help large organizations detect stealthy threat actors by flagging suspicious behaviors, especially when they employ fully undetected malware or legitimate tools. EDRs can generate alerts upon execution of unpopular applications or legitimate tools known to be abused by attackers—for example, so-called living-off-the-land binaries (LOLBins)—thus allowing defenders to see and investigate suspicious activities happening in their networks.

Invisimole, a threat actor ESET researchers have been tracking for a few years, bears out its name, as it targets high-profile organizations for espionage purposes and deploys various strategies in order to be as difficult as possible to detect. Once Invisimole's operators have a foothold in an organization, they typically set up different persistence chains to ensure continued access. However, although different chains exist, they have one point in common: No malicious code is present on disk.

Further, Invisimole's operators abuse legitimate tools to load and decrypt, in memory, malicious tools that enable their espionage activities. The usage of these legitimate tools makes it hard for standard detection technologies to detect anomalies. In these cases, in which stealth is the ultimate goal, defenders relying on a properly configured EDR solution can detect such malicious activities and correctly mitigate attacks.

7

ENDPOINT DETECTION AND RESPONSE AT ESET

WHAT IS ENDPOINT DETECTION AND RESPONSE?

Endpoint detection and response (EDR) solutions collect and analyze large amounts of data generated from activity on endpoints. Suspicious behaviors produce an alarm that alerts security professionals to further investigate and potentially discover any attacks that would otherwise go unnoticed. ESET developed ESET Enterprise Inspector (EEI) as an EDR solution capable of protecting both Windows and macOS endpoints.

MITRE ATT&CK®

ESET Enterprise Inspector references its detections to the MITRE ATT&CK knowledge base of adversarial tactics, techniques and procedures, which provides comprehensive information about the most complex threats and adversary groups afflicting cyberspace. With over 20 contributions to the knowledge base and having participated in the third *MITRE Engenuity ATT&CK Evaluations*, our EDR solution is battle tested and mature.

Threat hunting

Packaged with a set of rigorously tested rules to detect suspicious behaviors and with advanced filtering capabilities to sort data based on file popularity, reputation, signature, behavior and other contextual information, EEI offers automated and easy threat hunting capable of discovering targeted attacks. Since EEI allows the creation of custom rules, and rule exclusions, it can be fine-tuned to make it best suited for an environment or to re-scan the events database with custom configurations for historic threat hunting.

Public API

ESET Enterprise Inspector features an API that allows security engineers to export detections, thus allowing effective integration with tools such as SIEM, SOAR, ticketing and other tools.

ABOUT ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit **www.eset.com** or follow us on **LinkedIn**, **Facebook**, and **Twitter**.

Contributing Editors:

Rene Holt, ESET PR Writer
James Shepperd, ESET PR Writer
Branislav Ondrasik, ESET Security Research Communications Manager

Additional Contributions From:
WeLiveSecurity
ESET Creative Studio

CYBERSECURITY
EXPERTS ON YOUR SIDE