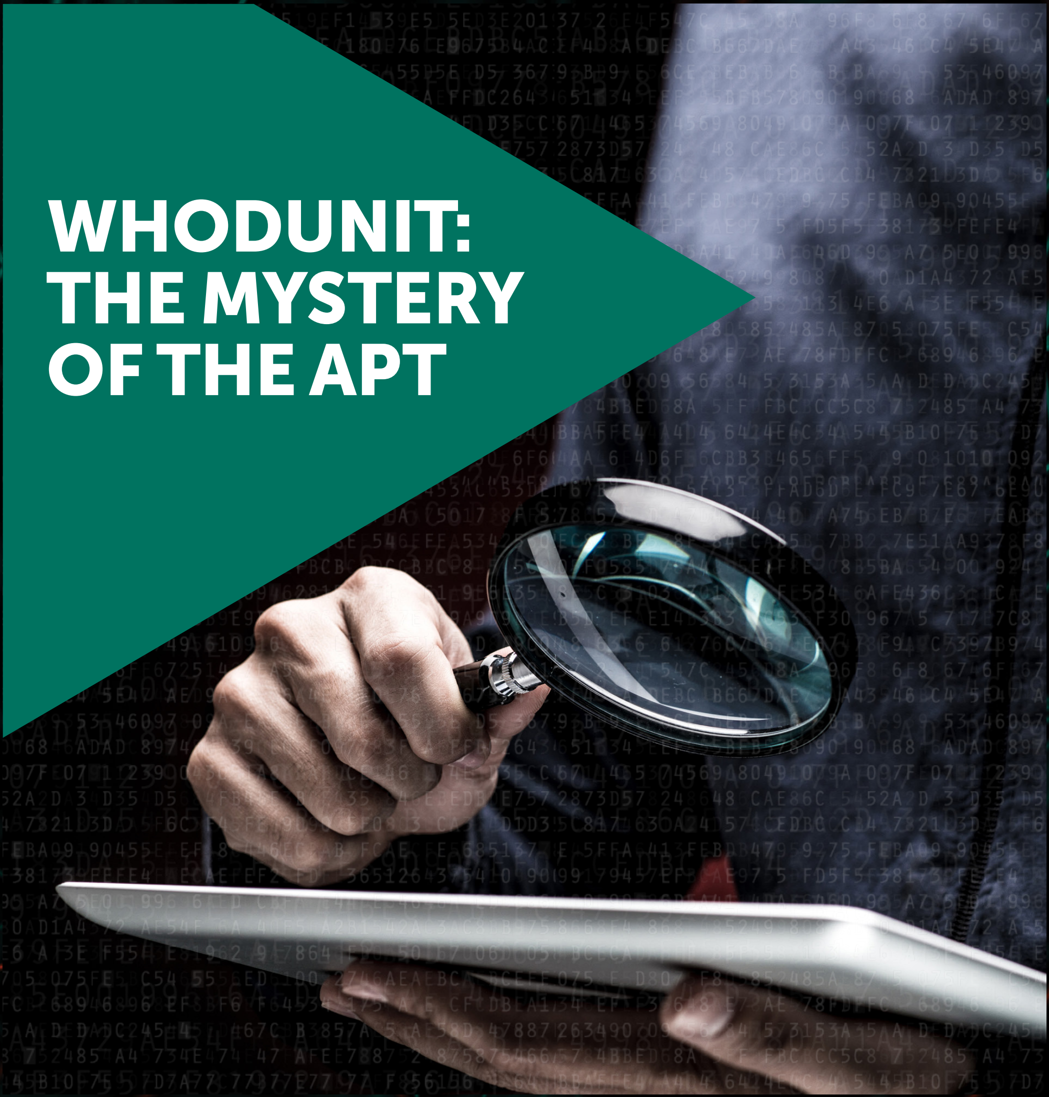
SECURITY SPOTLIGHT

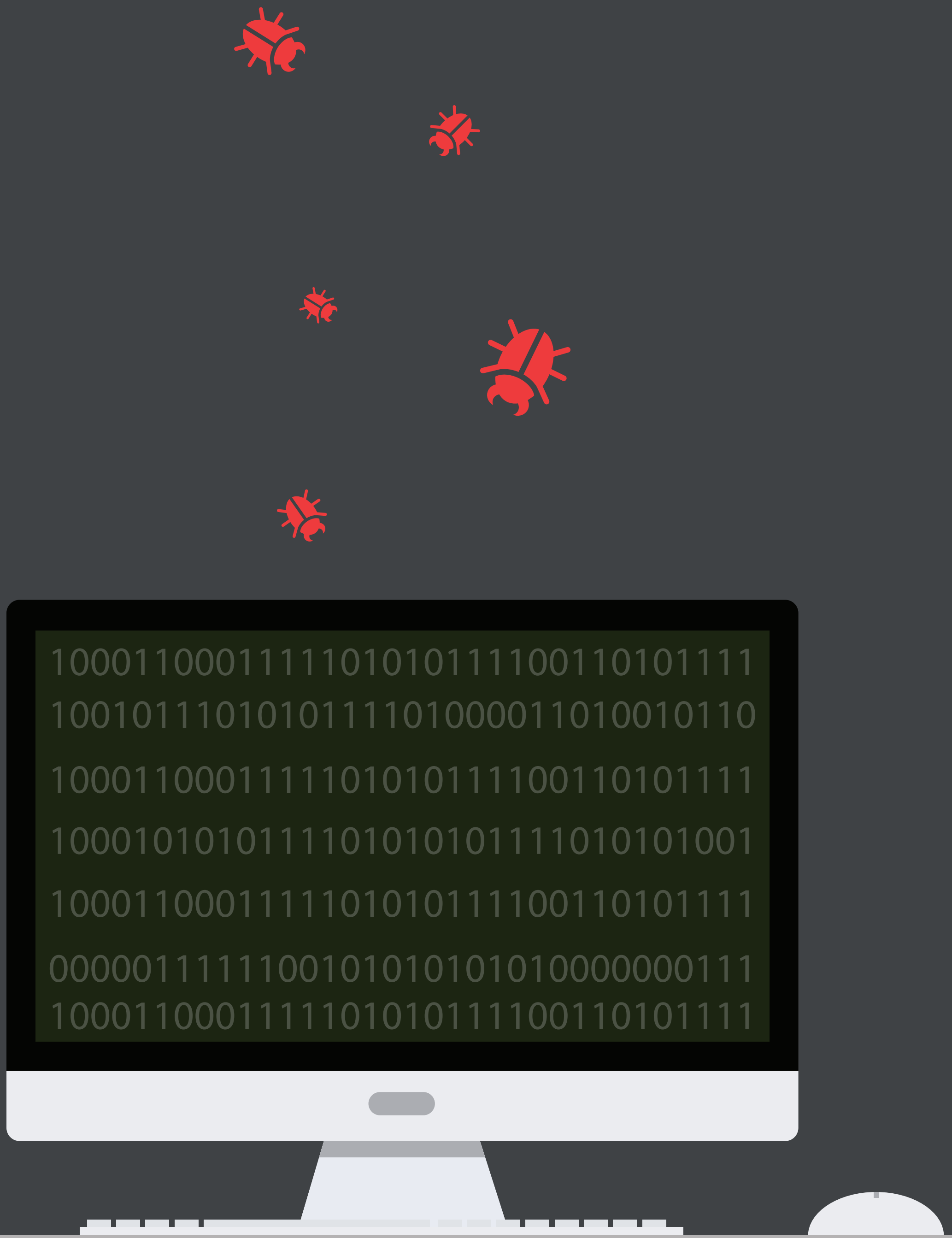
WHODUNIT: THE MYSTERY OF THE APT



KASPERSKY lab

Cybercriminals can be certain about a few things.

- Most companies store their important data on their networks. Patents, innovative designs, customer information, and confidential data — it's all there.
- Intellectual property is highly valuable, making it the number one thing cybercriminals target.
- Many companies don't understand the latest security practices and don't install the latest patches on their security products, leaving an open door for cybercriminals to steal what matters most.
- You don't have to be a large government agency or an energy company to be an attractive target. Every company, no matter how small, has sensitive data that can be stolen and re-sold.
- This is a growing and lucrative market.



For companies that experienced a targeted attack, 68% report data loss or exposure as a direct result of the attack.[1]

What is an APT?

Advanced Persistent Threats (APTs) are complex attacks, consisting of many different components. Using penetration tools, such as spear phishing messages or exploits, network propagation mechanisms, spyware, and rootkits or bootkits to conceal their presence, APTs are designed with one objective in mind: **gaining undetected access to sensitive information**.

What's in a name?

APTs are "advanced" because the tools used in these attacks are more sophisticated than those usually used by cybercriminals. They are "persistent" because once an organization is breached, it can remain in the system for months or even years. In fact, according to a study by HP and Mandiant, the median amount of time before a company detects a data breach is 205 days, leaving cybercriminals with months of access to sensitive data before they are discovered.

Search and destroy

Because APTs make up just 1% of the threat landscape, they are rare but incredibly costly to any company. Given all of this, shouldn't threat intelligence researchers be able to find APTs easily and spend the time and resources figuring out how to block them? Furthermore, shouldn't it be easy to figure out who did it and go after the threat actor?

Not so fast.

While APTs are highly complex, it is possible to discover them and name them, which makes up the bulk of the work that the threat intelligence community does. However, **it is almost impossible to say with complete certainty who carried out an attack**.

The threat intelligence work that we do at Kaspersky Lab is complex, time-consuming and filled with pitfalls and sometimes false leads, but few things are more complex than figuring out who carried out an attack. For this reason, **we at Kaspersky Lab are attribution agnostic**, meaning that we will never claim with 100% certainty to know who a threat actor is.

We do, however, conduct in-depth and thorough analysis of every APT we study to learn how the threat landscape is changing, what methods are being employed, and how companies can protect themselves. In the end, the data and intelligence we gain from this research proves to be highly valuable and helps us to do what we set out to do—protect companies and their data from these advanced and damaging attacks.

[1] Corporate *IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

Preventing targeted attacks is the biggest, most concerning future challenge – cited by 45% of firms.[2]

What makes attribution so difficult?

Attribution—or the naming of threat actors—is a multi-faceted issue that cannot be oversimplified. For one thing, **the stakes of pointing the finger at any one group are high**. Get it wrong, and your reputation is on the line. Worse yet, if a victim, such as a government entity, takes it upon themselves to "hack back," then your misattribution can be costly.

Beyond the problem of naming the wrong group, attribution has other problems and pitfalls that make it much more difficult than it may seem at first appearance. Some APTs are truly perplexing with no clear indicators that point in any one direction. Other times, because they feel they can act with impunity, operators become careless and provide more data than they should or reuse infrastructure from previous attacks. They may even leave a trail to an IP address or reuse a handle that has lots of personal information. Either way, the indicators of compromise can take up a wide range of possibilities, and figuring out which direction to go in adds to the complexity of naming a threat actor.

Finally, it is important to note the motive behind naming a threat actor. For some inexperienced threat intelligence (TI) producers, the loud and unverifiable claims may make good public relations in the short term, but they can reveal a level of naiveté that does not help the threat intelligence community as a whole. **Sharing verifiable threat intelligence is an important part of the TI community, and it is important that it is as accurate and well-vetted as possible.**

[2] Corporate *IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

How do we study APTs?

Studying APTs is complex, time-consuming—and at times, perplexing and frustrating. But it is never dull. Our work involves digging into large amounts of metadata and following the trail of clues. In particular, we look at patterns revealed by the following:

- Languages used in the code
- Times when the malware was compiled
- Motivation behind the attacks
- Types of targets
- IP addresses used during the attack
- Where the data was sent to after the attack

All of it forms a matrix of data points that can be used to determine potential threat actors and how they operate.

Timestamps

Timestamps are a digital record of when a particular event took place. Although timestamps can be altered with ease, many samples usually include original times that can give us an understanding of an actor's toolkit throughout the years.

With a large enough collection of related samples, it is also possible to create a timeline of the campaign operator's workday, allowing us to pinpoint a general timezone for their operations.

Strings, debug paths and metadata

Even the most innocuous strings used to operate the normal functions of a backdoor can point to the malware authors. The most obvious one is the preferred language of the threat actor where certain colloquial shortcomings can indicate one region over another.

A favorite indicator of threat researchers is the debug path, a string describing the folder structure leading up to the files from the time of development that made its way into the final binary. Debug paths often reveal a username or may even reveal internal naming conventions.

Phishing documents are often filled with metadata that sometimes include the original user handles and unintentional information from the save state that points to the machine of the original author.

Infrastructure and backend operations

Command-and-control infrastructure can be costly and difficult to maintain, so even well-resourced attackers have a tendency to reuse infrastructure between teams, allowing us to see sharing between the same threat actor cluster.

Backend connections are those that take place when an attacker retrieves data from an exfiltration server or email account, prepares a staging or phishing server, or checks on a compromised domain to ensure its availability. Usually, attackers use an anonymizing service like Tor, but mistakes do happen, allowing us a window to look into.

Toolkits

Malware Families

Most advanced threat actors take the time to build their toolkits and develop custom backdoors and exploits. These actors guard their well-designed toolkit carefully, which allows researchers to hone in on a threat actor, knowing they oversee a tightly controlled malware family.

However, malware ownership is not static, and the ownership can be transferred. We see malware being shared with other actors in the same cluster or source code being leaked to other actors.

Code Reuse

Malware developers will often reuse specific pieces of code that have worked well in the past, allowing researchers to hone in on the specific traits of a threat actor.

Passwords

Believe it or not, even advanced threat actors reuse passwords. We see them deploying droppers with password-protected resources, protecting seemingly unrelated malware families with the same password, and even using protecting hard-coded encryption keys from different malware families with the same password.

Zero Days

The presence of a zero-day immediately sets a threat actor apart and tells us we are dealing with an advanced and well-resourced attacker. Many advanced attackers have exploit developers in house with some threat actors unleashing what seems like an unlimited supply of exploits. When it appears that a zero-day exploit is released in separate and unrelated incidents within the same timeframe, then this kind of code sharing likely indicates the same actor or cluster of actors.

Tasking

An important part of threat intelligence is looking into the chosen targets themselves and asking key questions. What geopolitical conflicts in the “real world” may be motivating the attack? Can we map the APT campaign to a specific geopolitical or regional situation? However, since tasking is largely interpretive and can be oversimplified, it must be used judiciously.

APT Investigations

A few ground rules about attribution

As we have noted, Kaspersky Lab is attribution agnostic, meaning that we will never claim with absolute certainty to know who a threat actor is. In our process of discussing examples of threat actors, it is often necessary to point to commonly held beliefs as to the origin of certain threat actors. However, these are not our own assertions or claims. **We remain steadfast in our conviction that attribution is a complex issue where researchers cannot claim 100% certainty about the provenance of a threat actor.**

For a more in-depth look at our approach to attribution, we recommend that you read our whitepaper, *Wave Your False Flags!: Deception Tactics Muddying Attribution in Targeted Attacks*.

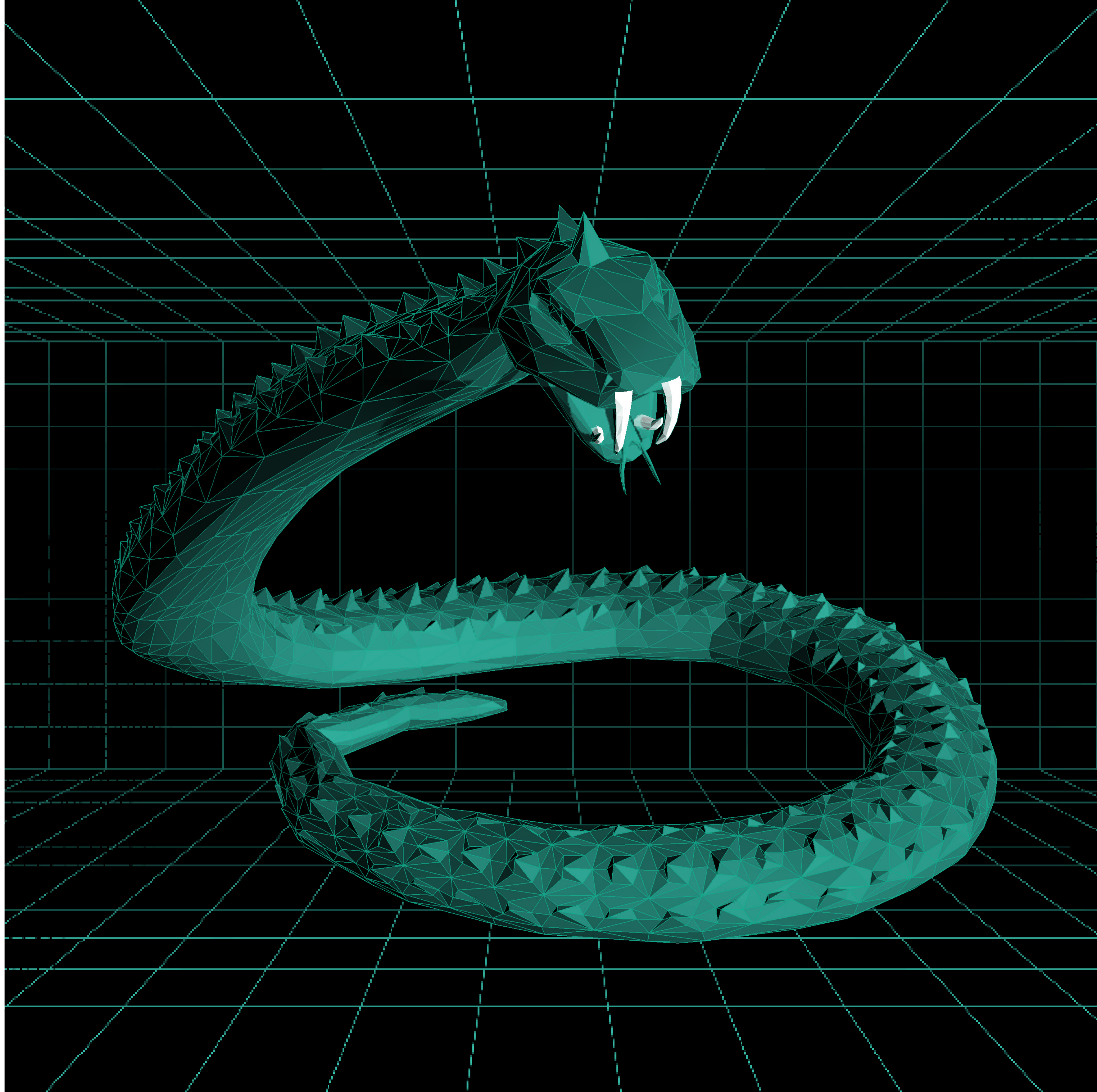
With that in mind, we would like to introduce you to some APTs that have been particularly interesting to research.

Turla

Turla APT group, also known as Snake and Uroboros, is one the most advanced threat actors in the world whose language artifacts indicate that they are Russian speakers. Kaspersky Lab's research uncovered some previously unknown findings about its operations.

Turla is especially difficult to track, not only because of its complex tools, but also because of its use of a satellite-based command-and-control mechanism. Command-and-control servers are the base for advanced cyberattacks, but they are also the weakest link in malicious infrastructure. Because researchers can use C&C servers to trace attackers back to their physical locations, most threat actors are careful to hide them as deeply as possible in their infrastructure.

In the case of Turla, they chose quite an effective method to conceal their C&C server—by hiding the servers' IPs in the sky. By using a one-way satellite-based internet connection, they identify active IP addresses that they can use to communicate, going through a number of steps to mask their location. For more on our research into the Turla group and how it operates, you can read our blog or our in-depth article on Securelist.



Sofacy

Sofacy, also known as Fancy Bear, is a Russian-speaking advanced threat group that has been active since at least 2008, targeting primarily military and government agencies worldwide.

In recent years, Sofacy has displayed even more advanced tools in its arsenal. Using multiple backdoors, the APT infects a target with several different malicious tools, one of which serves as a reinfection tool in case another one is blocked or killed by a security solution.

The attackers also use modularization, which puts some features of the backdoors into separate modules in order to hide malicious activity. In many recent attacks, Sofacy made use of a new version of its USB-stealing implant, which allows it to copy data from air-gapped computers. While using a USB storage device is often considered outdated in the modern threat landscape, the danger presented by these devices is still very real.

What is most interesting about Sofacy is its effectiveness in conducting deception operations in an effort to maintain a level of plausible deniability. For more information on other instances in which Sofacy is believed to have employed a false front in order to mask its intentions, we recommend reading our whitepaper, *Wave Your False Flags!: Deception Tactics Muddying Attribution in Targeted Attacks*.

For more on our research into the Sofacy group and how it operates, you can read our blog or the in-depth article on Securelist.

Duqu 2.0

First discovered in 2011 by *CrySyS* Lab and extensively researched by Kaspersky Lab's *GReAT* (Global Research and Analysis Team), Duqu was initially notorious for its malware's relationship to Stuxnet. We can say without hesitation that Duqu is one of the most skilled and powerful APT groups out there.

The organization behind Duqu is careful to stay under the radar. In 2015, it used three zero-day exploits, which indicates vast resources. In order to stay hidden, the malware resides in kernel memory only and does not directly connect to a command-and-control server, making it hard for anti-malware solutions and researchers to detect.

Duqu 2.0 has been used to attack a complex range of targets of geopolitical interest. Victims have been found in Western, Middle Eastern and Asian countries. Infections have been linked to the P5+1 events and venues related to the negotiations with Iran about a nuclear deal. This threat actor also launched a similar attack in relation to the 70th anniversary event of the liberation of Auschwitz-Birkenau.

More details on Duqu 2.0 can be found in our whitepaper, *Duqu 2.0: Frequently Asked Questions*. In order to mitigate the threat, Kaspersky Lab released Indicators of Compromise (IOC) and offered its assistance to all interested organizations.

You can find more details about Duqu 2.0 in our press release on the topic and an in-depth article on Securelist. Our whitepaper, *Wave Your False Flags!: Deception Tactics Muddying Attribution in Targeted Attacks* also has details on the malware traits it exhibited.

It's Complicated

APTs pose a direct threat to businesses and organizations worldwide, making our research into them a pressing issue for companies of all sizes.

For those that have experienced a targeted attack on their networks, 68% suffered data loss or exposure as a direct result. 22% lost access to customer-facing services, and 21% of these incidents affected suppliers that they share data with. The ripple effects of an attack go far beyond just the infected device or server. Your customers, your clients and your suppliers can all feel the immediate effects of such an attack.

APTs are also something that affects businesses of every size. In our survey, targeted attacks were listed in the top five of contributing factors to cyberincidents across all size business sectors.

But there is hope.

Knowledge is a powerful tool. Guided by our research, Kaspersky Lab uses this intelligence to improve our security solutions and help our customers worldwide understand how to protect themselves. Our research not only helps customers to stay on top of the latest threats but also serves to add to the body of research throughout the threat intelligence community, something that helps all businesses to stay ahead of the threats that pose the biggest risks.

In our recent global survey of more than 4,000 companies worldwide, 80% cite data loss or exposure due to targeted attacks among their top security concerns.

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at usa.kaspersky.com/business-security

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about our advanced cybersecurity solutions, particularly our endpoint products and our other IT security solutions and services.
usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab