kaspersky BRING ON THE FUTURE

What financial organizations need to know about APTs: current actors, challenges and tactics

The Financial Services industry is the number one target for cyber criminals everywhere. This includes attacks on financial institutions themselves, as well as attacks on their customers.

While the motivations behind cyber-attacks may vary, there is one constant – the motivation of financial gain. Any organization that holds or controls funds of any kind will always be a top target for cyber criminals. What's more, the bigger the bounty, the further the criminals will go in order to steal it.

It's unsurprising that APT and APT-like attacks constitute a real and present threat to the finance industry. Consider the scale of the malice, stealth, tradecraft and tenacity required to sneak inside an organization's network and move laterally within it while avoiding detection for a dwell time that reaches into several months. APT groups are far removed from the lone wolves simply relying on mass market cybercrime to make a quick buck.

The threat that APTs post to the financial sector is so grave that in February of 2020, the MITRE ATT&K framework announced that it would be evaluating commercial cybersecurity tools on the basis of their efficacy in the face of the Carbanak APT. Carbanak is a threat group that mainly targets banks – the name also refers to the malware the group uses. Some Carabank attacks are tracked separately under the designation Fin7, but we believe that the groups are intimately related as they use the same Carabank code . Carabank has haunted the finance sector for some eight years, stealing over $1bn US. What's more, the group puts the persistent into APT – even though some members were arrested in 2018, they (and their code) continue to threaten the finance sector.

Here's a short list of some of the key APT groups that pose a threat to the financial sector today:

1. Lazarus, an APT group with strong links to North Korea, is sometimes known as BlueNoroff, HIDDEN COBRA, or Zinc. This year, the group has expanded its repertoire, using Magecart 3.0 code for digital payment-card skimming, and branching out into ransomware with VHD. In 2016, Lazarus stole $81million from one victim alone in their attack on the Bank of Bangladesh.
2. MuddyWater attacks a wide range of targets in the telco, governmental, diplomatic, education, finance, healthcare, NGO and logistics sectors. They too have followed the trend of branching out into ransomware. MuddyWater are known for using the common APT PowerShell backdoor tactic, together with a growing range of other tools and code, including Python RATs and proprietary tools in C#.
3. Sodinokibi, sometimes known as REVil uses a range of APT-like tactics, including VPN exploitation (entry), Mimikatz (credential theft) and PsExec (for reconnaissance and lateral movement). The group was behind a large attack on a Chilean bank in 2020.
4. Maze may have announced its retirement from cybercrime in November 2020, but banks would do well to learn from the group's tactics and rapid success (over only 18 months), which could very well inspire copycat attacks. Among its victims were Xerox, Canon, Cognizant and the state-owned Banco de Costa Rica. When Banco de Costa Rica refused to pay the ransom, Maze announced that they would be publishing one stolen customer database a week online, adding: "We regret that Banco BCR and regulators don't care about their clients and their personal data." Banco de Costa Rica is not the only Maze victim to have been humiliated by Maze leaking its customer data online.

A note on ransomware:
Over the past few months (see below), APT groups have increasingly 'diversified their portolios' by branching out into ransomware. The chilling thing about ransomware is that we can never be certain of the exact number (or identity) of its targets because those who pay the ransom don't show up in lists of known victims. Financial organizations simply cannot afford the reputational damage cost they would incur should it become known that they have fallen victim to a ransomware attack.
However, paying the ransom could soon have severe consequences – in October of 2020, the US Department of the Treasury issued a stern advisory stating **that the payment of ransoms to cyber criminals could constitute a breach of Office of Foreign Assets Control (OFAC) sanctions**. We expect other governments to follow suit as ransomware becomes a growing international problem.

Key APT challenges

Stealth
The stealth that characterizes APT and APT-like attacks poses an enormous challenge, even for large IT-matured organizations. Discovery alone is not enough, and proactive hunting, informed by up-to-date sector-specific Threat Intelligence is essential, particularly with some security systems producing a useless bombardment of highly distracting, time-wasting, false alerts.

Persistence
APT attackers are persistent and patient, moving laterally within a network for weeks or months on end, carrying out reconnaissance and setting up multiple backdoors before taking any noticeable action.

Exploitation of siloed infrastructure, security and even culture
APT groups know that large organizations are weakened by siloes in their infrastructure, cyber defences and even culture. Siloes can stymie joined-up thinking across departments, IT vendors, as well as databases and other tools. APT groups exploit this disjointedness: stealth is easier when victims are unable to form a clear, visible big picture of what is truly going on across their infrastructure.

Lack of context
Accurate, contextual, relevant and up-to-date threat intelligence is absolutely critical for financial organizations seeking to prevent, discover and respond to the presence of APTs in their networks. At a macro level, that threat intelligence must include a broad understanding of the APT landscape in relation to the finance sector.

The cybersecurity talent gap
To put a positive spin on it, now is a good time to encourage your children to take up a career in cybersecurity. But the reality for today is not so shiny. There simply isn't enough cybersecurity talent available, making recruitment and retention extremely challenging. APT groups know that their expertise often exceeds that of in-house cybersecurity teams, and it's no surprise that ego is often cited as one of the key drivers of cybercriminal activity.

So what can financial organizations do about it?

The first step is to understand that even the most highly IT-matured organizations are not expected to tackle APT and APT-like attacks alone. It's a global problem, constantly shifting across regions and sectors, and a team would need at least talent, relevant threat intelligence and time to carry out the research and response tasks necessary for defending an organization against such a growing and shifting threat.

We encourage all of our IT-matured enterprise customers to ensure that they diligently address what we see as the three pillars of any successful anti-APT security strategy. Namely, security teams must be:

- **Equipped:**
  Cybersecurity is one area of expertise where even a skilled worker can legitimately blame their tools. Protection from multivector attacks and APTs requires a unified consolidated platform that gives total visibility, eliminating obstructive siloes and preventing 'alert fatigue' and other routine tasks within the incident response process.
- **Informed:**
  The existing advanced expertise of IT-matured organizations must never be taken for granted. After all, the cybercrime horizon is constantly shifting and expanding. Ongoing education and powerful threat intelligence from reliable cybersecurity partner are absolutely crucial.
- **Reinforced:**
  Should an APT be discovered, even the most advanced IT security analysts should have access to external support for 3rd party insight, security assessment, managed threat hunting and incident response. While APTs are usually highly targeted, they rarely target only one victim. External expertise can shed a multi-sector global light on the likely paths of an APT, and deliver actionable advice on the most decisive way to eliminate it from the system.

At Kaspersky we understand the challenges involved in defending against APTs and similar threats. That's why we've built a unified concept that fulfils the three pillars of a successful anti-APT security strategy. **Kaspersky Expert Security** allows your team to make short work of sophisticated threats and APT-like attacks, meeting the challenges of stealth, persistence, siloes and talent head on. It's designed and built around Extended Detection and Response (XDR) platform and packed with features that augment the in-house superpowers of your IT security team, including comprehensive threat intelligence, training and expert guidance.

Find out more about **Kaspersky Expert Security**

Kaspersky Expert Security

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven. Transparent. Independent.