Kaspersky Security Bulletin. 2016 Predictions

It's the end of the world for APTs as we know it

By Juan Andrés Guerrero-Saade, GReAT on November 17, 2015. 4:03 pm

KASPERSKY SECURITY BULLETIN

APT CYBERCRIME DATA PROTECTION FINANCIAL MALWARE HACKERS RANSOMWARE

Download PDF version

Download EPUB

Introduction

As the year comes to an end, we have an opportunity to take stock of how the industry has evolved and to cast our predictions for the coming years. Taking advantage of a rare global meeting of our GReAT and Anti-Malware Research experts, we tossed ideas into the ring and I have the privilege of selecting some of the more noteworthy and plausible for both the coming year and the long-term future as we foresee it. The outlook for our rapidly evolving field of study is quite thought-provoking and will continue to present us with interesting challenges. By sticking to sober metrics, perhaps we can skip the usual science fiction fear mongering and come to some accurate predictions for both the short- and long-term.

No more APTs

Before you start celebrating, we should point out that we're referring to the 'Advanced' and 'Persistent' elements – both of which the threat actors would gladly drop for overall stealth. We expect to see a decrease in the emphasis on persistence, placing a greater focus on memory-resident or fileless malware. The idea will be to reduce the traces left on an infected system and thus avoid detection altogether. Another approach will be to reduce the emphasis on advanced malware. Rather than investing in bootkits, rootkits, and custom malware that gets burned by research teams, we expect an increase in the repurposing of off-the-shelf malware. Not only does this mean that the malware platform isn't burned upon discovery but it also has the added benefit of hiding the actor and his intentions in a larger crowd of mundane uses for a commercially available RAT. As the shine of cyber-capabilities wears off, return on investment will rule much of the decision-making of state-sponsored attackers – and nothing beats low initial investment for maximizing ROI.

APT: a decrease in the emphasis on persistence, a focus on memory-resident or fileless malware #KL2016Prediction

The nightmare of ransomware continues

We expect to see the success of Ransomware spread to new frontiers. Ransomware has two advantages over traditional banking threats: direct monetization and relatively low cost per victim. This amounts to decreased interest from well-resourced third-parties such as banks, as well as low levels of reporting to law-enforcement agencies. Not only do we expect ransomware to gain

ground on banking trojans but we also expect it to transition into other platforms. Weak attempts at bringing ransomware to mobile (Simplelocker) and Linux (Ransom.Linux.Cryptor, Trojan-Ransom.FreeBSD.Cryptor) have already been witnessed, but perhaps the more desirable target platform is OS X. We expect ransomware to cross the Rubicon to not only target Macs but also charge 'Mac prices'. Then, in the longer term, there is the likelihood of IoT ransomware, begging the question, how much would you be willing to pay to regain access to your TV programming? Your fridge? Your car?

> We expect ransomware to gain ground on banking trojans and to transition into other platforms #KL2016Prediction

Betting against the house: financial crimes at the highest level

The merging of cybercrime and APT has emboldened financially motivated criminals who have gracefully transitioned from attacking end users to going after the financial institutions themselves. The past year has seen plenty of examples of attacks on point-of-sale systems and ATMs, not to mention the daring Carbanak heist that pilfered hundreds of millions of dollars. In the same vein, we expect cybercriminals to set their sights on novelties like alternate payment systems (ApplePay and AndroidPay) whose increasing rate of adoption should

offer a new means of immediate monetization. Another inevitable point of interest is stock exchanges, the true mother lode. While frontal attacks may yield quick payoffs, we mustn't overlook the possibility of more subtle means of interference, such as going after the black-box algorithms employed in high-frequency trading to ensure prolonged gains with a lower likelihood of getting caught.

Cybercriminals will set sights on novelties like alternate payment systems and stock exchanges #KL2016Predictio n

Attacks on security vendors

As attacks on security vendors rise, we foresee an interesting vector in compromising industry-standard reverse-engineering tools like IDA and Hiew, debugging tools like OllyDbg and WinDbg, or virtualization tools like the VMware suite and VirtualBox. CVE-2014-8485, a vulnerability in the Linux implementation of 'strings', presents an example of the vulnerable landscape of nontrivial security research tools that determined attackers may choose to exploit when targeting researchers themselves. In a similar vein, the sharing of freeware research tools through code repositories like Github is an area ripe for abuse, as users will more often than not pull code and execute it on their systems without so much as a glance. Perhaps we should also be casting a suspicious glance towards popular implementations of PGP so eagerly embraced by the infosec community.

We foresee a vector in

Tweet

compromising reverse-engineering, debugging & virtualization tools #KL2016Predictio n

Sabotage, extortion and shame

From dumps of celebrity nudes to the Sony and Ashley Madison hacks and the HackingTeam dump, there has been an undeniable increase in DOXing, public shaming, and extortion. Hacktivists, criminals, and state-sponsored attackers alike have embraced the strategic dumping of private pictures, information, customer lists, and code to shame their targets. While some of these attacks are strategically targeted, some are also the product of opportunism, taking advantage of poor cybersecurity to feign hacker prowess. Sadly, we can only expect this practice to continue to rise exponentially.

Whom do you trust?

Perhaps the scarcest commodity in the current internet age is trust. Abuse of trusted resources will further drive this scarcity. Attackers will continue to enlist open-source libraries and whitelisted resources for malicious purposes. We expect another form of trust to be abused, that of a company's internal resources: as crafty attackers seek to expand their foothold on an infected network, they may target resources limited to the company intranet such as waterholing Sharepoint, file server, or ADP portals. Perhaps we'll even witness the furthest extension of the already rampant abuse of trusted certificates as attackers establish an entirely fabricated certificate authority to issue certificates for their malware.

Tweet

Attackers will enlist open-source libraries and whitelisted resources for malicious purposes #KL2016Prediction

APT actors down the road

The profitability of cyberespionage has not escaped the attention of our foes and, as we expected, mercenaries have begun populating the scene. This trend will only increase to match the demand for cyber-capabilities by both companies as well as known APT actors looking to outsource less critical tasking without risking their tools and infrastructure. We could float the term ‘APT-as-a-Service’, but perhaps more interestingly we can expect the evolution of targeted attacks to yield ‘Access-as-a-Service’. The latter entails the sale of access to high-profile targets that have already fallen victim to mercenaries.

Tweet

We'll see members of well-established APT teams potentially coming out of the shadows #KL2016Prediction

Looking further into the future of cyberespionage, we see

members of well-established APT teams ('APT 1%ers', if you will) potentially coming out of the shadows. This would happen in one of two forms: as part of the private sector with the proliferation of 'hacking back', or by sharing their insights with the larger infosec community, perhaps by joining us at conferences to share the other side of the story. In the meantime, we can expect the APT Tower of Babel to incorporate a few more languages.

The future of the Internet

The infrastructure of the internet itself has shown signs of tension and cracks in recent years. Concerns over massive router botnets, BGP hijacking and dampening, DNS attacks en masse, or server-powered DDoSes betray a lack of accountability and enforcement on a global scale. Looking further down the line to long-term predictions, we can consider what the internet might look like if that narrative of a globally connected village continues to wither. We may end up with a balkanized internet divided by national borders. At that point, concerns over availability may come down to attacks on the service junctures that provide access between different sections, or perhaps geopolitical tensions that target the cables that connect large swathes of the internet. Perhaps we'll even see the rise of a black market for connectivity. Similarly, we can expect that as technologies that power the internet's underbelly continue to gain mainstream attention and widespread adoption, developers with a stake in shadow markets, exchanges, and forums are likely to develop better technologies to keep the underground truly underground.

Tweet

The internet's cracked: we may end up with a balkanized internet divided by national borders

#KL2016Predictio
n

The future of transportation

As investment and high-end research capabilities are dedicated to developing autonomous vehicles for both personal and commercial distribution, we will witness the rise of distributed systems to manage the routes and traffic of large volumes of these vehicles. The attacks may not focus on the distribution systems themselves, but perhaps on the interception and spoofing of the protocols they rely on (a proof of concept of the vulnerabilities of the widely adopted Global Star satcom system was presented by a Synack researcher at this year's BlackHat conference). Foreseeable intentions behind these attacks include theft of high-value goods or kinetic damage resulting in loss of life.

Crypto: a breakdown in the reliability of standards and a need of 'post-quantum cryptography' #KL2016Predictio
n

The cryptopocalypse is nigh

Finally, we cannot overemphasize the importance of cryptographic standards in maintaining the functional value of the internet as an information-sharing and transactional tool of unparalleled promise. These cryptographic standards rely on the expectation that the computational power required to break their encrypted

output is simply above and beyond our combined means as a species. But what happens when we take a paradigmatic leap in computational capabilities as promised by future breakthroughs in quantum computing? Though quantum capabilities will not be initially available to the common cybercriminal, it signals a breakdown in the reliability of current crypto-standards and a need to design and implement 'post-quantum cryptography'. Given the poor rate of adoption or proper implementation of high-quality cryptography as it is, we do not foresee a smooth transition to counterbalance cryptographic failures at scale.

Related Articles