KASPERSKY lab

Kaspersky Security Bulletin

PREDICTIONS FOR 2017: 'INDICATORS OF COMPROMISE' ARE DEAD

GREAT

CONTENTS

Yet another year has flown past and, as far as notable infosec happenings are concerned, this is one for the history books. Drama, intrigue and exploits have plagued 2016 and, as we take stock of some of the more noteworthy stories, we once again cast our gaze forward to glean the shapes of the 2017 threat landscape. Rather than thinly-veiled vendor pitching, we hope to ground these predictions in trends we've observed in the course of our research and provide thought-provoking observations for researchers and visitors to the threat intelligence space alike.

OUR RECORD

Last year's predictions fared well, with some coming to fruition ahead of schedule. In case you didn't commit these to memory, some of the more notable predictions included:

APTs: We anticipated a decreased emphasis on persistence as well as an increased propensity to hide in plain sight by employing commodity malware in targeted attacks. We've seen this, both with an increase in memory or fileless malware as well as through the myriad reported targeted attacks on activists and companies, which relied on off-the-shelf malware like NJRat and Alienspy/Adwind.

Ransomware: 2016 can be declared the year of ransomware. Financial malware aimed at victimizing users has practically been galvanized into a ransomware-only space, with the more effective extortion scheme cannibalizing malware development resources from less profitable attempts at victimizing users.

More Bank Heists: When we considered the looming expansion of financial crime at the highest level, our hypothetical included targeting institutions like the stock exchange. But it was the attacks on the SWIFT network that brought these predictions to bear, with millions walking out the door thanks to crafty, well-placed malware.

Internet Attacks: Most recently, the oft-ignored world of sub-standard Internet-connected devices finally came to bear on our lives in the form of a nasty IoT botnet that caused outages for major Internet services, and hiccups for those relying on a specific DNS provider.

Shame: Shame and extortion have continued to great fanfare as strategic and indiscriminate dumps have caused personal, reputational, and political problems left and right. We must admit that the scale and victims of some of these leaks have been genuinely astonishing to us.

WHAT DOES 2017 HAVE IN STORE?

Those dreaded APTs

The rise of bespoke and passive implants

As hard as it is to get companies and large-scale enterprises to adopt protective measures, we also need to admit when these measures start to wear thin, fray, or fail. Indicators of Compromise (IoCs) are a great way to share traits of already known malware, such as hashes, domains, or execution traits that will allow defenders to recognize an active infection. However, the trendsetting one-percenters of the cyberespionage game have known to defend against these generalized measures, as showcased by the recent ProjectSauron APT, a truly bespoke malware platform whose every feature was altered to fit each victim and thus would not serve to help defenders detect any other infections. That is not to say that defenders are entirely without recourse but it's time to push for the wider adoption of good Yara rules that allow us to both scan far-and-wide across an enterprise, inspect and identify traits in binaries at rest, and scan memory for fragments of known attacks.

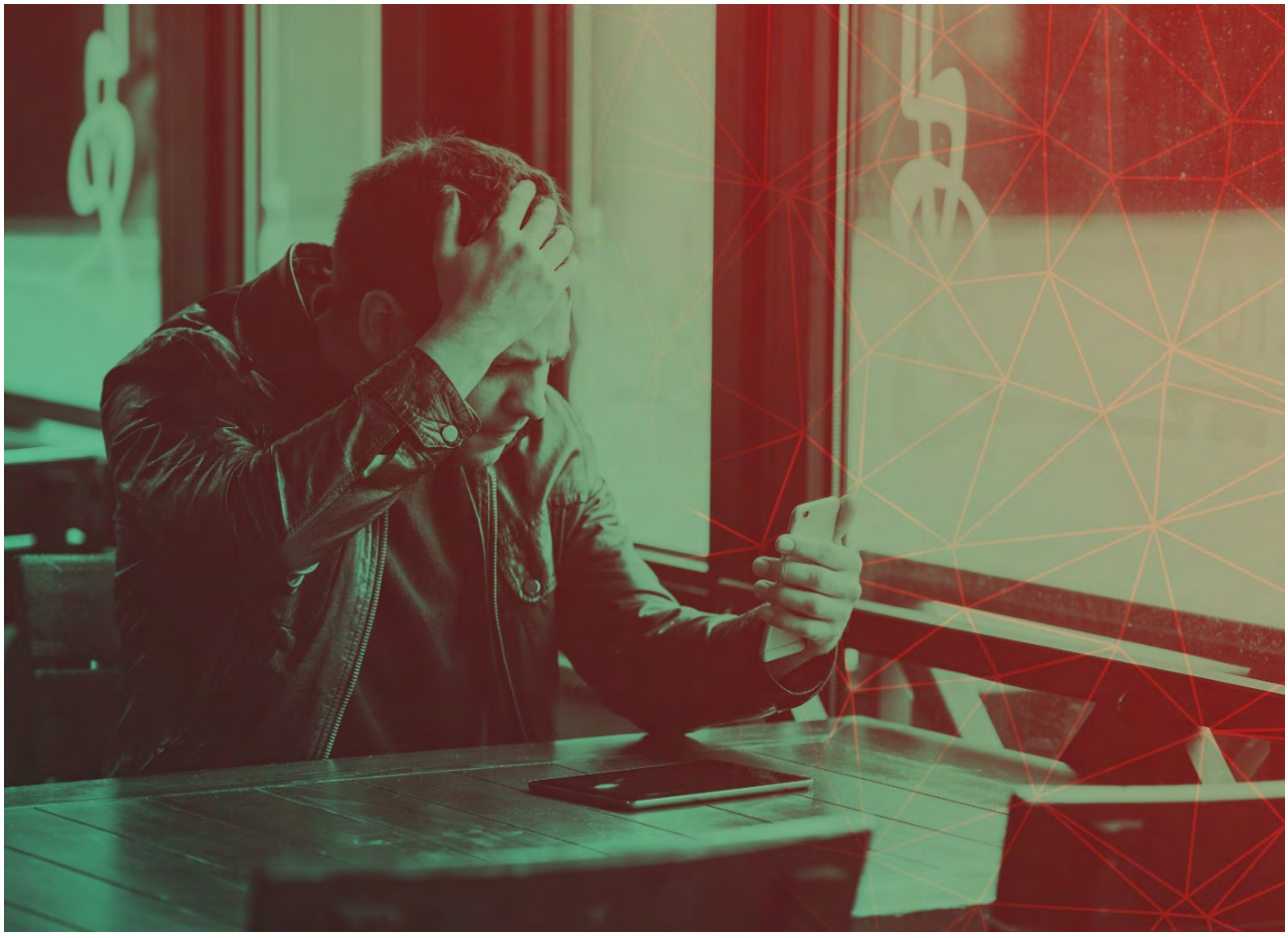
ProjectSauron also showcased another sophisticated trait we expect to see on the rise, that of the 'passive implant'. A network-driven backdoor, present in memory or as a backdoored driver in an internet gateway or internet-facing server, silently awaiting magic bytes to awaken its functionality. Until woken by its masters, passive implants will present little or no outward indication of an active infection, and are thus least likely to be found by anyone except the most paranoid of defenders, or as part of a wider incident response scenario. Keep in mind that these implants have no predefined command-and-control infrastructure to correlate and provide a more anonymous beachhead. Thus, this is the tool of choice for the most cautious attackers, who must ensure a way into a target network at a moment's notice.

Ephemeral infections

While adoption of PowerShell has risen as a dream tool for Windows administrators, it has also proven fruitful ground for the gamut of malware developers looking for stealthy deployment, lateral movement, and reconnaissance capabilities unlikely to be logged by standard configurations. Tiny PowerShell malware stored in memory or in the registry is likely to have a field day on modern Windows systems. Taking this further, we expect to see ephemeral infections: memory-resident malware intended for general reconnaissance and credential collection with no interest in persistence. In highly sensitive environments, stealthy attackers may be satisfied to operate until a reboot wipes their infection from memory if it means avoiding all suspicion or potential operational loss from the discovery of their malware by defenders and researchers. Ephemeral infections will highlight the need for proactive and sophisticated heuristics in advanced anti-malware solutions (see: System Watcher).

Espionage goes mobile

Multiple threat actors have employed mobile implants in the past, including Sofacy, RedOctober and CloudAtlas, as well as customers of HackingTeam and the suspected NSO Pegasus iOS malware suite. However, these have supplemented campaigns largely based on desktop toolkits. As adoption of Desktop OS's suffers from a lack of enthusiasm, and as more of the average user's digital life is effectively transferred to their pockets, we expect to see the rise of primarily mobile espionage campaigns. These will surely benefit from decreased attention and the difficulty of attaining forensic tools for the latest mobile operating systems. Confidence in codesigning and integrity checks has stagnated visibility for security researchers in the mobile arena, but this won't dissuade determined and well-resourced attackers from hunting their targets in this space.



The future of financial attacks

We heard you'd like to rob a bank...

The announcement of this year's attacks on the SWIFT network caused uproar throughout the financial services industry due to its sheer daring; measured in zeros and commas to the tune of multi-million dollar heists. This move was a natural evolution for players like the Carbanak gang and perhaps other interesting threat actors. However, these cases remain the work of APT-style actors with a certain panache and established capability. Surely, they're not the only ones interested in robbing a bank for sizable funds?

As cybercriminal interest grows, we expect to see the rise of the SWIFT-heist middlemen in the well-established underground scheme of tiered criminal enterprises. Performing one of these heists requires initial access, specialized software, patience, and, eventually, a money laundering scheme. Each of these steps has a place for already established criminals to provide their services at a fee, with the missing piece being the specialized malware for performing SWIFT attacks. We expect to see the commodification of these attacks through specialized resources being offered for sale in underground forums or through as-a-service schemes.

Resilient payment systems

As payment systems became increasingly popular and widely adopted, we expected to see greater criminal interest in these. However, it appears that implementations have proven particularly resilient, and no major attacks have been noted at this time. This relief for the consumer may, however, entail a headache for the payment system providers themselves, as cybercriminals are wont to target the latter through direct attacks on the payment system infrastructure. Whether these attacks will result in direct financial losses or simply outages and disruption, we expect increased adoption to attract more nefarious attention.

Dirty, lying ransomware

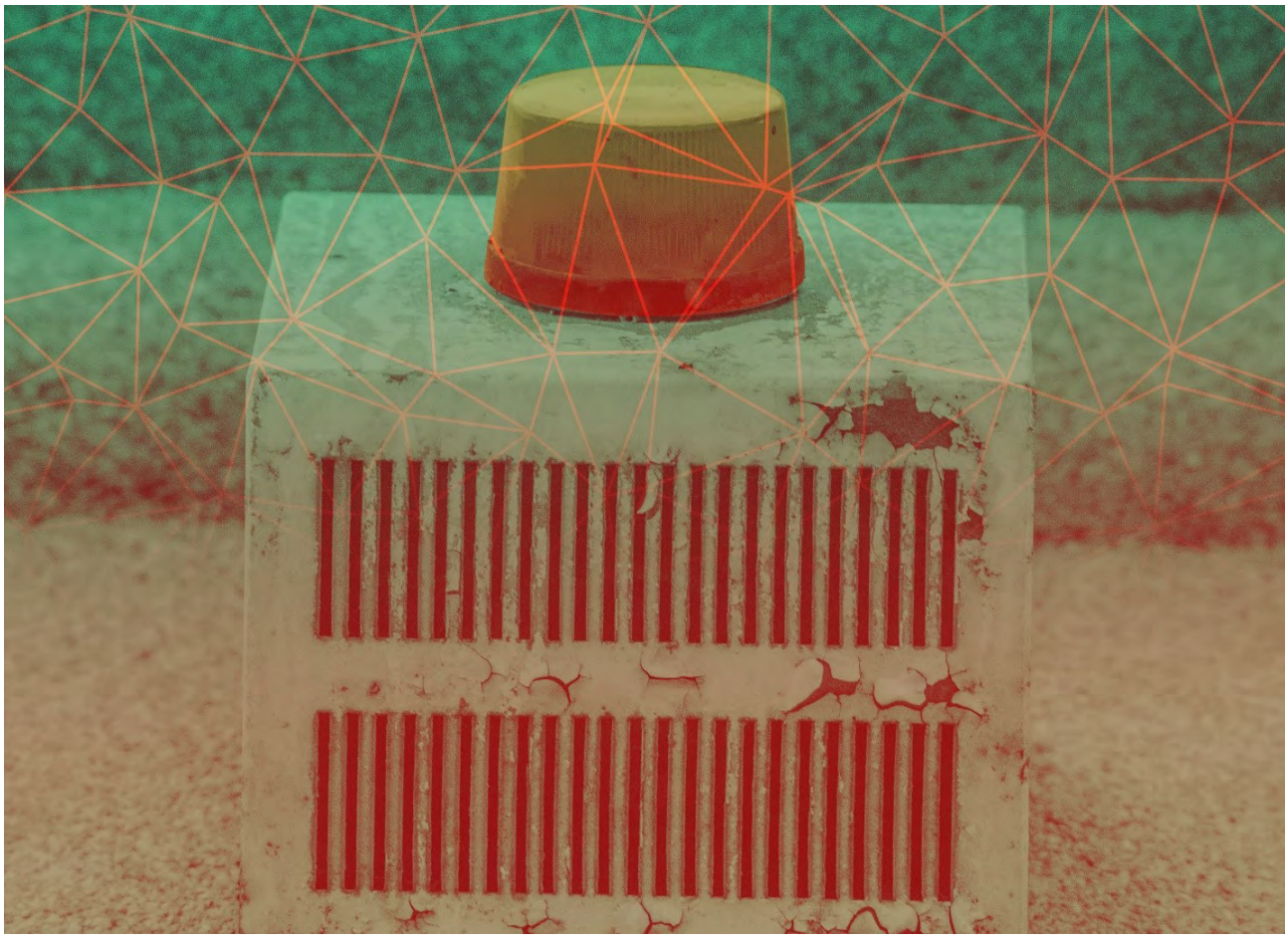
As much as we all hate ransomware (and with good reason), most ransomware thrives on the benefit of an unlikely trust relationship between the victim and their attacker. This criminal ecosystem relies on the tenet that the attacker will abide by a tacit contract with the victim that, once payment is received, the ransomed files will be returned. Cybercriminals have exhibited a surprising semblance of professionalism in fulfilling this promise and this has allowed the ecosystem to thrive. However, as the popularity continues to rise and a lesser grade of criminal decides to enter the space, we are likely to encounter more and more 'ransomware' that lacks the quality assurance or general coding capability to actually uphold this promise.

We expect 'skiddie' ransomware to lock away files or system access or simply delete the files, trick the victim into paying the ransom, and provide nothing in return. At that point, little will distinguish ransomware from wiping attacks and we expect the ransomware ecosystem to feel the effects of a 'crisis of confidence'. This may not deter larger, more professional outfits from continuing their extortion campaigns, but it may galvanize forces against the rising ransomware epidemic into abandoning hope for the idea that 'just pay the ransom' is viable advice for victims.

The big red button

The famous Stuxnet may have opened a Pandora's Box by realizing the potential for targeting industrial systems, but it was carefully designed with a watchful eye towards prolonged sabotage on very specific targets. Even as the infection spread globally, checks on the payload limited collateral damage and no industrial Armageddon came to pass. Since then, however, any rumor or reporting of an industrial accident or unexplained explosion will serve as a peg to pin a cyber-sabotage theory on.

That said, a cyber-sabotage induced industrial accident is certainly not beyond the realm of possibility. As critical infrastructure and manufacturing systems continue to remain connected to the internet, often with little or no protection, these tantalizing targets are bound to whet the appetite of well-resourced attackers looking to cause mayhem. It's important to note that, alarmism aside, these attacks are likely to require certain skills and intent. An unfolding cyber-sabotage attack is likely to come hand-in-hand with rising geopolitical tensions and well-established threat actors intent on targeted destruction or the disruption of essential services.



The overcrowded internet bites back

A brick by any other name

Long have we prophesied that the weak security of the Internet of Things (or Threats) will come back to bite us, and behold, the day is here. As the Mirai botnet showcased recently, weak security in needlessly internet-enabled devices provides an opportunity for miscreants to cause mayhem with little or no accountability. While this is no surprise to the infosec-aficionados, the next step may prove particularly interesting, as we predict vigilante hackers may take matters into their own hands.

The notion of patching known and reported vulnerabilities holds a certain sacrosanct stature as validation for the hard (and often uncompensated) work of security researchers. As IoT-device manufacturers continue to pump out unsecured devices that cause wide-scale problems, vigilante hackers are likely to take matters into their own hands. And what better way than to return the headache to the manufacturers themselves by mass bricking these vulnerable devices? As IoT botnets continue to cause DDoS and spam distribution headaches, the ecosystem's immune response may very well take to disabling these devices altogether, to the chagrin of consumers and manufacturers alike. The Internet of Bricks may very well be upon us.

The silent blinky boxes

The shocking release of the ShadowBrokers dump included a wealth of working exploits for multiple, major manufacturers' firewalls. Reports of exploitation in-the-wild followed not long after as the manufacturers scrambled to understand the vulnerabilities exploited and issue patches. However, the extent of the fallout has yet to be accounted for. What were attackers able to gain with these exploits on hand? What sort of implants may lie dormant in vulnerable devices?

Looking beyond these particular exploits (and keeping in mind the late 2015 discovery of a backdoor in Juniper's ScreenOS), there's a larger issue of device integrity that bears further research when it comes to appliances critical to enterprise perimeters. The open question remains, 'who's your firewall working for?'

Who the hell are you?

The topic of False Flags and PsyOps are a particular favorite of ours and to no surprise, we foresee the expansion of several trends in that vein...

Information warfare

The creation of fake outlets for targeted dumps and extortion was pioneered by threat actors like Lazarus and Sofacy. After their somewhat successful and highly notorious use in the past few months, we expect information warfare operations to increase in popularity for the sake of opinion manipulation and overall chaos around popular processes. Threat actors interested in dumping hacked data have little to lose from crafting a narrative through an established or fabricated hacktivist group; diverting attention from the attack itself to the contents of their revelations.

The true danger at that point is not that of hacking, or the invasion of privacy, but rather that as journalists and concerned citizens become accustomed to accepting dumped data as newsworthy facts, they open the door to more cunning threat actors seeking to manipulate the outcome by means of data manipulation or omission. Vulnerability to these information warfare operations is at an all-time high and we hope discernment will prevail as the technique is adopted by more players (or by the same players with more throwaway masks).

The promise of deterrence

As cyberattacks come to play a greater role in international relations, attribution will become a central issue in determining the course of geopolitical overtures. Governmental institutions have some difficult deliberating ahead to determine what standard of attribution will prove enough for demarches or public indictments. As precise attribution is almost impossible with the fragmented visibility of different public and private institutions, it may be the case that 'loose attribution' will be considered good enough for these. While advising extreme caution is important, we must also keep in mind that there is a very real need for consequences to enter the space of cyberattacks. Our bigger issue is making sure that retaliation doesn't engender further problems as cunning threat actors outsmart those seeking to do attribution in the first place. We must also keep in mind that as retaliation and consequences become more likely, we'll see the abuse of open-source and commercial malware begin to increase sharply, with tools like Cobalt Strike and Metasploit providing a cover of plausible deniability that doesn't exist with closed-source proprietary malware.

Doubling-down on False Flags

While the examples reported in the False Flags report included in-the-wild cases of APTs employing false flag elements, no true pure false flag operation has been witnessed at this time. By that we mean an operation by Threat Actor-A carefully and entirely crafted in the style and with the resources of another, 'Threat Actor-B', with the intent of inciting tertiary retaliation by the victim against the blameless Threat Actor-B. While it's entirely possible that researchers have simply not caught onto this already happening, these sorts of operations won't make sense until retribution for cyberattacks becomes a de facto effect. As retaliation (be it overtures, sanctions, or retaliatory CNE) becomes more common and impulsive, expect true false flag operations to enter the picture.

As this becomes the case, we can expect false flags to be worth even greater investment, perhaps even inciting the dumping of infrastructure or even jealously guarded proprietary toolkits for mass use. In this way, cunning threat actors may cause a momentary overwhelming confusion of researchers and defenders alike, as script kiddies, hacktivists, and cybercriminals are suddenly capable of operating with the proprietary tools of an advanced threat actor, thus providing a cover of anonymity in a mass of attacks and partially crippling the attribution capabilities of an enforcing body.

What privacy?

Pulling the veil

There's great value to be found in removing what vestiges of anonymity remain in cyberspace, whether for the sake of advertisers or spies. For the former, tracking with persistent cookies has proven a valuable technique. This is likely to expand further and be combined with widgets and other innocuous additions to common websites that allow companies to track individual users as they make their way beyond their particular domains, and thus compile a cohesive view of their browsing habits (more on this below).

In other parts of the world, the targeting of activists and tracking of social media activities that 'incite instability' will continue to inspire surprising sophistication, as deep pockets continue to stumble into curiously well-placed, unheard of companies with novelties for tracking dissidents and activists through the depth and breadth of the internet. These activities tend to have a great interest in the social networking tendencies of entire geographic regions and how they're affected by dissident voices. Perhaps we'll even see an actor so daring as to break into a social network for a goldmine of PII and incriminating information.

The espionage ad network

No pervasive technology is more capable of enabling truly targeted attacks than ad networks. Their placement is already entirely financially motivated and there is little or no regulation, as evidenced by recurring malvertising attacks on major sites. By their very nature, ad networks provide excellent target profiling through a combination of IPs, browser fingerprinting, and browsing interest and login selectivity. This kind of user data allows a discriminate attacker to selectively inject or redirect specific victims to their payloads and thus largely avoid collateral infections and the persistent availability of payloads that tend to pique the interest of security researchers. As such, we expect the most advanced cyberespionage actors to find the creation or co-opting of an ad network to be a small investment for sizable operational returns, hitting their targets while protecting their latest toolkits.

The rise of the vigilante hacker

Following his indiscriminate release of the HackingTeam dump in 2015, the mysterious Phineas Fisher released his guide for aspiring hackers to take down unjust organizations and shady companies. This speaks to a latent sentiment that the asymmetrical power of the vigilante hacker is a force for good, despite the fact that the HackingTeam dump provided live zero-days to active APT teams and perhaps even encouragement for new and eager customers. As the conspiratorial rhetoric increases around this election cycle, fuelled by the belief that data leaks and dumps are the way to tip the balance of information asymmetry, more will enter the space of vigilante hacking for data dumps and orchestrated leaks against vulnerable organizations.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy