Observations on Emerging Threats

Paul Ferguson
paul_ferguson@trendmicro.com
Senior Threat Researcher
Threat Research, Trend Micro, Inc.

USENIX LEET 2012

Trend Micro's Threat Research group is specially tasked with looking forward on the threat landscape and working with technology and/or various product development groups inside the company to ensure that, as a company, we deliver the appropriate security solutions to address emerging threats to our customers. To accomplish this requires our threat research group to understand, explore, and deconstruct various malicious technologies, campaigns, vulnerabilities, and exploits which are currently being perpetrated on victims today. With this in mind, I have briefly outlined below what we are currently witnessing as “emerging threats” which pose serious potential risks to our customers, and others in their daily use of the Internet and beyond.

Ongoing Evolution, Professionalization, and Commoditization of Exploit Kits. Recent trends suggest an increase in the ongoing development, evolution, and sophistication of exploitation tool kits, such as the Black Hole Exploit Kit. In fact, we have observed the number of domains which are being created to host these exploit kits have skyrocketed in the latter part of 2011, and we continue to see these kits being used as “weapon of choice” by cybercriminals. Also, these kits are becoming a commodity in the criminal underground, bought, bartered, and sold. This trend only serves to increase the victimization attack surface.

Increased Sophistication with Traffic Direction Systems (TDS). Traffic Direction Systems (TDS) are used as initial landing pages, also known as “doorway pages”, which direct traffic to content based on a variety of criteria such as operating system, browser version, user agent, and geographic location. Traffic Direction Systems can be dedicated to a criminal action (e.g. Koobface), or a standalone enterprise. Some TDS routing leads to legitimate sites and servers while others are used in criminal campaigns. A TDS dedicated to malicious activity can be used to manage traffic flow, track hit-count, the ongoing number of infected users, which affiliate is responsible for infected hosts, and are primarily used for monetization and management.

Smaller, More Diversified and Compartmentalized Botnets. We have also observed a trend insofar as to the size and scope of botnets. Instead of huge, monolithic botnets, criminals appear to have shifted to smaller, more compartmentalized botnet infrastructures. This approach has multiple benefits for the operators – primarily with regards to loss of infrastructure due to take-downs, domain suspension, and other mitigation techniques. With more compartmentalization, portions of the infrastructure may be disabled or dismantled without complete loss to the criminal. It also helps the smaller botnet size to go unnoticed as compared to a larger, “noisier” botnet.

Modularization. We have also observed a high degree of modularization in more advanced malware, especially banking Trojans and other malware related to bank account hijacking, etc. This is especially true with SpyEye, where the specific modules have been developed as “plug-ins” for specific functions, such as form-grabbers, back-connect (real-time, on-demand communications with the controller), and web-injects.

Evolution of Mobile Threats. Current mobile malware is almost “Proof of Concept” and almost non-existent outside of the Chinese Android market. We suspect it will increase dramatically when more e-commerce applications arrive with the next generation of handsets and NFC (Near-Field Communications) capabilities, which will significantly boost hand-held e-commerce point-of-sale (POS) transactions. This will spur the “professional” cybercriminals to take advantage of these opportunities as they are principally motivated by financial gain.

Continued Exploitation of Social Networks. There's a reason why cybercriminals continue to use the same social-engineering ploys over and over again – they work. Humans beings – in the majority of instances – seem to be vulnerable to very simple ploys aimed at compromising themselves. This susceptibility allows cybercriminals to plant Trojan Horse programs, backdoor access tools, and consistently continue to be successful in their widespread campaigns to carry out criminal campaigns. Social networks, such as Facebook, are considered "low-hanging fruit" for these criminals because of the sheer number of users, and the overall lack of technical security sophistication by the users of such services.

Hard Lessons Learned in Protecting Critical Infrastructure. Unfortunately, this is an area where some very hard lessons may be learned – the protection of critical infrastructure (CI) is an area where there is a lack of security experience and an excess of opportunity for attackers. Traditionally, Industrial Control Systems (ICS) infrastructure – such as those found in the oil & gas industry, electricity generation, transmission and distribution, transportation, manufacturing, etc. – have been closed-loop network, separated and unreachable from public networks (e.g. the Internet), using proprietary protocols, and special-purpose platforms. In the past decade, these isolated special-purpose systems have become more commoditized, using off-the-shelf hardware and software which makes them subject to the same threats as traditional information technology systems. Also, they are now interconnected to the Internet and other public networks, increasing their attack surface and possibility of compromise due to malicious & unauthorized access.

New Exploitation Vectors Introduced via HTML5. The coming of HTML5 adoption will enable a whole new set of attacks which the Internet community at-large is mostly not ready or completely unable to defend against. These new attack capabilities include extended the ability for click-jacking, port scanning using cross-origin requests or WebSockets, and the ability to use HTML5 to extend social engineering attacks with in-browser web notifications dialogue boxes. Another new HTML5 feature allows an attacker who has successfully injected JavaScript code into a site (e.g. from an XSS attack) to alter how the forms on that page behave, enabling form tampering. Geo-location is one of the most talked about features introduced in HTML5. As a security and privacy concern, a site must always ask a user's permission before being able to get access to this location information. However, as has been seen in the past with features such as Vista's user access control, Android's application permissions, and with invalid HTTPS certificates – security based on a user needing to make a decision rarely works out well. Once permission is given, that site can not only learn the victim's location, but also track that user in real-time as they move around. Also with HTML5, attackers can now create a botnet which will run on any OS, in any location, on any device. Being heavily memory-based, HTML5 barely touches the disk, making it difficult to detect with traditional file-based anti-virus. JavaScript code is also very easy to obfuscate, so network IDS signature will also have a very hard time. Finally, being web-based, it will easily pass through most firewalls.

More Data Breaches via Advanced Persistent Threats (APT). The reason why Advanced Persistent Threats (APT) continue to work is that the targeted individuals on the receiving end of the attack are always able to be social-engineered. The targets of an APT attacks typical receive a malicious email that appears to be from someone they know. Since the distribution is small – usually just a few members of a single organization – a unique malicious document can be created making it increasingly difficult for anti-virus products to ensure detection. Moreover, there is an increasing movement toward multiple stages of malware delivery that use different command and control servers in order to further frustrate defensive measures. The initial malware may be just a dropper that downloads an additional backdoor, often a RAT (Remote Access Trojan, or "back door" Trojan), through which the attackers can introduce tools used to increase their privilege and engage in lateral movement throughout the target's network. Ultimately, the attackers seek to collect and exfiltrate data, often email and documents, to location(s) under their control. The ex-filtration may take many forms, including being sent over HTTP and FTP, or through the File Transfer capability of RATs. However, APT malware is now increasingly using third-party encrypted services, such as Google's *GTalk*, for both command and control and data ex-filtration.

Efforts by Criminals to Host Services Out of Reach of Law Enforcement and Service Termination. Due to the increased pressure from law enforcement and other industry stakeholders in their efforts to police and prohibit cybercrime activities, we expect to see criminal efforts to move their infrastructure and hosting services to locations with less restrictive legal regimes. While the security industry and law enforcement focuses on disabling criminal infrastructure, attribution and arrests of criminal actors, and as various countries update their laws to further restrict and address these crimes, the "bullet-proof hosting" situation will get more difficult for cybercriminals to find. To maintain their revenue and operational continuity, it is highly likely that we will see more cybercrime being hosted in countries with newly emerging Internet infrastructure and hosting capabilities (e.g, Northern and Central Africa), yet with outdated or non-existent legal regimes to address these sorts of online crimes.

Summary

With the advent and evolution of new networking technologies, the threat and security landscape also shifts and changes. It is not that the emerging threat landscape is necessarily better or worse given this situation – yet it is critical to understand how it is changing in order to properly defend against these attacks, and put into place the appropriate security posture.