How to Thwart the Digital Insider – an Advanced Persistent Response to Targeted Attacks

A Trend Micro Opinion Piece
By Tom Kellermann, Vice President of Cyber Security, Trend Micro Inc.
August 2012

One of the oft-repeated themes in media reporting of cyber security events is that the "threat landscape is constantly evolving," that attacks are becoming increasingly sophisticated and targeted and the men and women behind them are better resourced than ever before. It's certainly true, but begs for a deeper and more nuanced analysis. How are these attacks getting more sophisticated? How can a digital insider lay hidden, undetected within an organization for years on end? And more importantly, how can advanced situational awareness help us to respond and mitigate these threats?

It should be acknowledged by now that traditional defences have already been rendered obsolete. Over 90 percent of enterprise networks contain active, malicious malware with one new threat created every second (Trend Micro research). Our increasingly cloud-based IT environments, which are being forced to cope with an influx of insecure endpoints in the form of employee-owned mobile devices, are proving a fertile ground for cyber criminals. Add to this the fact that well-organized criminal gangs are targeting their cyber attacks with more precision and sophistication than ever before and at a macro level you have all the ingredients for step change in modern threats.

"Over 90% of enterprise networks contain active, malicious malware with one new threat created every second."

Trend Micro Research

What makes the process even easier for the cyber criminals is that individuals or groups can download modularized, automated code from underground sites to carry out sophisticated, targeted attacks. Make no mistake about it, this weapons bazaar of cyber space has democratized the means to carry out these attacks, extending them beyond the hands of the mercenaries who first created them, and if you're one of the Fortune 500 assume your firm is already in the cross-hairs.

Over the past six years we have heard many horror stories regarding APTs (Advanced Persistent Threats), however the advanced cyber kill chains associated with APTs is no longer a monopoly of regimes as these targeted attacks have become privatized. In the end the APT is just a delivery mechanism for that digital insider. Once inside, the big problem is not just that it will try and maintain command and control, but that it will propagate, exfiltrate data and above all seek to maintain and sustain itself hidden from view. This latter characteristic is what makes such targeted attacks so pernicious – their ability to evade detection.

The attackers know full well that if organizations are alerted to a breach, IT is likely to check for two things – any vulnerabilities which a hacker might have exploited to gain network access, and signs of communication with an unknown IP address. Both incident responses can be foiled. Firstly, the digital insider will make sure that once they have infiltrated a network they patch any vulnerabilities – this is partly to disguise their own entry route and

partly to ensure rival hackers do not piggy back on their efforts. They'll also clean up any malware to make sure it doesn't interfere with the assignment in hand.

Secondly, command and control will be moved inside the ecosystem and put on a 'sleep cycle' so that there is no constant and easily detectable 'umbilical' connection to a single IP address outside the organization. The digital insider will reach out, perhaps once a week or even once a month, to an outside IP address to avoid detection – as was noted with the recent Ixeshe campaign.

The bad guys are subverting common incident response strategies in an even more insidious way, as seen with the Flashback Mac Trojan attack. It involves the use of a specialized technique designed to prevent security researchers from running and analyzing the malware in their labs. Host identity-based encryption encrypts modules of the malware with keys based on information taken from the victim's machine, effectively tying the malware to that computer and making any analysis in a different environment particularly arduous.

So these are the advanced techniques cyber criminals are using to maintain and sustain their digital insider within a victim organization while data is being exfiltrated. This is a new and sophisticated threat which requires an advanced persistent response predicated on organizations gaining advanced situational awareness in real-time. Firms need to be able to spot the unwanted intruder and then increase the level of discomfort to the point where the adversary flees in search of easier prey.

Gaining this kind of advanced situational response requires organizations to look both outside and inside their networks. Firstly, they need to grasp the importance of big data analytics in being able to correlate and associate the various nuances of cyber crime campaigns occurring in the wild with what's going on inside the network. This kind of smart data modelling and analysis should be able to spot if there are any correlations between cyber attack activity on the Internet and an organization's IP addresses, users, domains and networks, giving them the information they need to act.

Secondly, organizations need to focus on multi-level rule-based event correlation of the sort featured in Trend Micro's own APT-hunter tool Deep Discovery. It's another vital piece of functionality in the armoury designed to spot unusual activity. Remember, these guys are past masters at lying hidden for years on end so we need to up our own game to achieve advanced situational awareness. It will require patience once a digital insider is discovered, however, and more monitoring to ascertain all of the actors behind a particular threat so that law enforcement can take over – this is not a time to go in all guns blazing.

In short, times have changed. Advanced targeted threats are within the reach of most capable cyber criminals and we need to forget about building castles in cyber space to keep them out. Assume you have been compromised and then begin to build an advanced persistent response. This is a change from what most IT teams are used to but it's a necessary one and vendors like Trend Micro, which uses big data analytics and multi-level rule-based event correlation capabilities, are here to help.

Ultimately it will require an unprecedented level of awareness of what's going on inside your network and the ability to correlate events happening outside to detect the intruder. Then it's all about building a better dungeon to contain that intruder, turning up the discomfort levels until they are forced to leave. Happy hunting.

Tom Kellermann
VP of Cyber Security
Trend Micro.

As Vice President of Cyber Security at Trend Micro, Mr. Kellermann is focused on acting as a trusted cybersecurity advisor and strategist within the federal, state and local government markets. He utilizes his experience as a security evangelist and government affairs expert to forge strategic partnerships both domestically and internationally, and increase Trend Micro's profile in emerging technologies and policy issues.

Tom Kellermann served as a Commissioner on The Commission on Cyber Security for the 44th Presidency and serves on the board of the International Cyber Security Protection Alliance (ICSPA). He sits on many boards including: the National Board of Information Security Examiners Panel for Penetration Testing, the Information Technology Sector Coordinating Council, and the Information Technology Information Sharing and Analysis Center (IT-ISAC) subcommittee on International Cybersecurity policy.

Mr. Kellermann is a Professor at American University's School of International Service and is a Certified Information Security Manager (CISM).

Formerly holding the position as Chief Technology Officer and Chief Cyber Strategist at AirPatrol Corporation, Tom Kellermann also spent five years as Vice President of Security Awareness for Core Security.

Previously, he was the Senior Data Risk Management Specialist for the World Bank Treasury Security Team, where he was responsible for internal cyber-intelligence and policy and for advising central banks around the world about their cyber-risk posture and layered security architectures. Along with Thomas Glaessner and Valerie McNevin, he co-authored the book "E-safety and Soundness: Securing Finance in a New Age."

Mr. Kellerman is also Trend Micro's representative on the The National Cyber Security Alliance (NCSA).

TREND MICRO™

Securing Your Journey to the Cloud