Tiger

Last Updated: Monday September 28, 2015

By Paul Roberts

A report from the security firm Trend Micro claims that targeted attacks against US firms have resulted in the theft of intellectual property on a massive scale – including 58 gigabytes of data from a single target. But how?

A report from the security firm Trend Micro is raising alarms about the threat of massive data theft from western corporations at the hands of skilled cyber adversaries, many based in China.

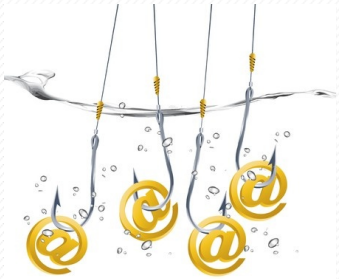
The report: Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors (PDF) was released this week and paints a grim picture of a long running and expansive campaign of cyber espionage that encompassed political and human rights organizations in the Asia Pacific region, as well as high tech and defense firms in the U.S.

According to Trend, the campaign combined a number of well-known tools in an orchestrated effort to steal massive troves of online data. The total haul, Trend estimates, could amount to terabytes of data, including full Active Directory e-mail dumps, intellectual property, strategic planning

Free Trial Gartner MQ Report Contact Us

How did attackers m ume of data out of victim organizations? The Iron Tiger report is something of a roadmap to the various high- and low tech means that sophisticated adversaries are employing today to subvert security and monitoring tools. According to Trend, the attackers behind Iron Tiger used extensive research on target organizations, followed by spear-phishing email messages to trick targeted individuals within that organization to install malicious software. Messages targeted VIPs within the organization including executives and engineers, as well as public relations and communications officers.

Once they had a foothold within target organizations, attackers would install back door programs on Microsoft Exchange servers and other data choke points. Exfiltration strategies ranged from the simple (renaming stolen files to fool filters looking for ZIP and RAR extensions) to the subtle. In a trend that is becoming more common, the attackers relied on common administrative tools to aid in the theft of data, so as not to arouse suspicion. For example: the attackers used the Robocopy



SHARE THIS ARTICLE

Digital Guardian Data Loss Prevention

Read how Digital Guardian for DLP gives you everything you need to stop sensitive data from getting out of your organization.

Read now

RELATED ARTICLES

Deus ex Machina: Securing Industrial Control Systems
The critical infrastructure that we rely on every day is becoming increasingly vulnerable to attack. What can be done to secure these systems?

7 Tips to Stop Falling for Phishing Attacks
Follow these helpful tips

application to extract stolen files from a server to a machine they controlled. PowerShell was used to export Exchange mailboxes, which were then encrypted and renamed prior to exfiltration.

Rest assured: malware played a key role in these compromises. The attackers used variants of common malware platforms like PlugX and Ghost. But the attackers also relied on custom hacking tools to access and remotely control target networks. Common web services such as Blogspot and Google Cloud provided a Command and Control platform for malware, using the solid reputations of those sites to cover for malicious activity within the network.

China appears to be the source of the Iron Tiger campaign, and Trend presents convincing evidence that ties the attackers to that country and, possibly, to individuals working within the cyber underground there. Whether those individuals are acting at the behest of the Chinese Communist Party, Chinese military, cyber criminal gangs or private concerns isn't known.

What is the solution? The unfortunate conclusion of the Iron Tiger is that there are no easy answers. The report makes clear that industrial and political cyber espionage are all part of a continuum and rely on many of the same tactics.

Attackers will build targeted attacks on top of long term reconnaissance. Convincing spear phishing e-mail messages make eventual infection of endpoints on target networks inevitability.

"Targets face serious repercussions, given the sensitive nature of the data they keep. The data the actors stole, after all, translates to years of invaluable government and corporate research and development (R&D) dollars," the report notes.

The proper response, then, is to boost efforts to detect on-going or nascent campaigns that target your organization – or even organizations like yours. Threat intelligence needs to be part of the solution, so you have an ear to the ground. But just as important are tools and strategies to spot unusual or suspicious information flows out of your network. That might be unusual file transfers ('What's that 100MB CSS or TXT file about?') or instances of known but unexpected tools like Robocopy or PowerShell.

Detect and prevent has been dead for a long time. The Trend Micro report makes clear what a complex science data leak prevention has become.

Paul F. Roberts is the Editor in Chief of The Security Ledger *and Founder of The* Security of Things Forum.

to get better at recognizing and avoiding phishing attacks.

Managing Cyber Risks in an Interconnected World
PwC Cyber Expert Looks at the Key Findings of the 2015 Global State of Information Security Survey

Comments

Please post your comments here

Your name *

As you would like it displayed

E-mail

The content of this field is kept private and will not be shown publicly.

Comment *

Submit

Privacy Policy

© DIGITAL GUARDIAN BY VERDASYS 2015