17 SEP 2015 NEWS

Iron Tiger Campaign Stolen 'Terabytes' of Data in APAC and US

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

Security researchers have discovered another advanced China-based targeted attack campaign which shifted its focus from APAC targets in 2013 to steal up to terabytes of data from hi-tech US government contractors.

"Emissary Panda" or "Threat Group-3390 (TG-3390)" launched its Iron Tiger campaign in 2010, spying on political targets and government agencies in China, Hong Kong, the Philippines and Tibet, according to Trend Micro.

The security vendor explained in a new report:

"The actors have stolen emails, full Active Directory dumps, intellectual property, strategic planning documents, and budget- or finance-related content—all of which can be used to sabotage target governments' or private organizations' plans."

The huge geographical shift to US government contractors in aerospace, energy, intelligence, nuclear engineering, and telecoms indicates that Iron Tiger "is part of a bigger campaign where specific targets are assigned to various teams," the report claimed.

The actors involved are said to be China based for several reasons.

The VPN servers they used were mainly located in China; file names and passwords, as well as some text resources and language IDs used in malware, were in simplified Chinese; several domains were found to be located in China; and other resources used including QQ, Lofter, and 163.com are used mainly in the Middle Kingdom.

Although the hackers are said to be "skilled computer security experts" they've not needed to pull out the full repertoire of advanced techniques as target networks were poorly protected, Trend Micro claimed.

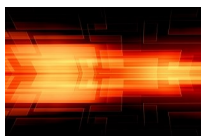
That said, they frequently used customized hacking tools like dnstunserver – which is apparently not available to buy on any darknet forum – and well-known RAT malware such as PlugX and Gh0st.

They also utilize consumer-facing platforms, including setting up C&C servers on Blogspot, and connecting a Gh0st variant to Chinese blogging platform Lofter.

Why Not Watch?

15 JUN 2015

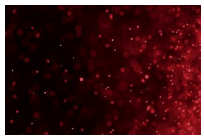
APTs: Overhyped or Under-managed?



9 JUL 2015

How Outsiders Become Insiders: Understanding and Combating Today's Threats

8 OCT 2015, 15:00 BST, 10:00 EDT



26 MAR 2015

A stolen code-signing cert from Korean security firm SoftCamp was used to move laterally inside target networks and circumvent security tools.

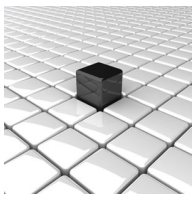
"To get deeper into networks, they intercept Microsoft Exchange credentials using Robocopy and the 'Export-Mailbox' PowerShell command—both unique means. They also use a Trojan that was specifically designed to only work on the Google Cloud Platform," the report revealed.

Spear phishing lures are typically aimed at targets ranging from execs to government officials, engineers to PR officers – with the subject matter of the email designed to pique the interest of a targeted individual.

Trend Micro also claimed the Iron Tiger attackers went to great lengths to avoid being hacked themselves, even patching a compromised C&C server by logging in as an admin and issuing a fix.

Given that the data stolen translates into "years of invaluable government and corporate research and development (R&D) dollars," organizations must do more to install multi-layered custom protection to better spot spear phishing and signs of intrusion, the report concluded.

Recommended for you



The Dark Side of Cryptography: Kl...
www.infosecurit...

Password Cracker Cracks 55 Charac...
www.infosecurit...

DDoS Weapon Found Hidden in...
www.infosecurit...

Peeling the Onion – Tor's Criminal...
www.infosecurit...

AddThis

0 Comments Infosecurity Magazine Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON INFOSECURITY MAGAZINE WHAT'S THIS?

Oracle CSO's Tone-Deaf Rant on Bug-Hunting Both Patronizing and ...
2 comments • a month ago
Billy — Oracle didn't create Java, Sun Microsystems did.....

Biometrics: Swapping Privacy for Sort-of Security
2 comments • a month ago
Editor — Slack Alice replies "Well, BBVA is the firm that is predicting that retinal scans will soon take off. This article ...

Phishing Education Can Save Nearly $4m Annually
1 comment • 22 days ago
Jason W. Strong — Security awareness training needs to be conducted by a professional who understands the in's ...

Networking Biz Ubiquiti Transfers $46.7 Million to Fraudsters
1 comment • a month ago
Kevin O'Brien — Best wishes to the Ubiquiti team on this. If anything, the attack highlights how reliance upon user ...

your site Privacy

Fighting Cyber-Attacks Through Security Intelligence

Insights into Incident Response - A View from the Front Lines

Related to This Story

Hackers Mix Old and New in Q1 Attacks

Trend Micro: Arid Viper Could be the Start of Something Big

Pawn Storm Spyware Hits Non-Jailbroken iOS Devices

Targeted Attacks Set to Go Mainstream in 2015

Emissary Panda Targets US Military Info

What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

1. 16 SEP 2015 NEWS
   Cisco Router Malware is Major New Targeted Attack Threat
2. 16 SEP 2015 NEWS
   New Malware Soars 43% to Reach 21 Million in Q2
3. 16 SEP 2015 NEWS
   BT Tests Banks with New Ethical Hacking Service
4. 25 OCT 2012 NEWS
   Jester's warbag: be careful of what you do on the internet
5. 15 SEP 2015 NEWS
   FBI in Internet of Things Cybersecurity Warning
6. 17 SEP 2013 NEWS
   OSINT: You Don't Need to Work for the NSA or GCHQ to Spy on People

Our website uses cookies

Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing Infosecurity Magazine, you agree to our use of cookies.

Okay, I understand Learn more

Copyright © 2015 Reed Exhibitions Ltd.