informa

InformationWeek IT NETWORK | Dark Reading | Network Computing | About Us | Advertise | Register | Login to your account | Welcome Guest

DARKReading | SIGN UP FOR OUR NEWSLETTERS | Search Dark Reading

Authors | Slideshows | Video | Tech Library | University | Radio | Calendar | Black Hat News | Follow DR:

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

ANALYTICS

10/13/2015
07:45 PM

Kelly Jackson Higgins
News
Connect Directly

0 COMMENTS
COMMENT NOW

Login
50% 50%

Like
Tweet
Share

Prolific Cybercrime Gang Favors Legit Login Credentials

FireEye researchers shed more light on infamous cybercriminals associated with RawPOS malware. and christen it 'FIN5.'

FIREEYE CYBER DEFENSE SUMMIT -- Washington, D.C. -- No 0days. No spearphishing, either: The cybercriminal group tied to numerous payment card breaches including Goodwill and best known by its so-called "RawPOS" malware employed legitimate user credentials to access its targets' networks.

Researchers at FireEye here today shared their recent findings on this prolific and long-running cybercrime gang that has been the subject of multiple Visa security alerts to merchants. The RawPOS memory scraper malware has been infecting the lodging industry in epidemic proportions over the past year, and is considered one of the first memory scrapers to target point-of-sale systems.

FireEye has dubbed the cybercrime gang FIN5. "One of the most unique things about FIN5 is that in every intrusion we responded to where FIN5 has been active, legitimate access was identified. They had valid user credentials to remotely log into the network," said Barry Vengerik, principal threat analyst at FireEye. "No sexy zero-days, no remote exploits -- not even spearphishing. They had credentials from somewhere."

FIN5, which earlier this year was profiled by researchers at Trend Micro and has been in action since at least 2008, uses real credentials from the victim organization's virtual private network, Remote Desktop Protocol, Citrix, or VNC. Vengerik says the attackers got those credentials via third parties associated with the victims' POS systems.

"Most of the maintenance and administration of POS systems are done by a third party -- the maintenance, patching, troubleshooting" is done remotely via those credentials, he said.

"FIN5 maintained access to two or more payment processor networks primarily for the goal of logging into and accessing their customers' environments," he said. "It's a textbook case of a lateral compromise between companies based on trust."

FireEye last year investigated a massive breach at a casino hotel with 1,200 endpoints that suffered losses to more than 150,000 payment cards. Vengerik declined to name the hotel.

The casino attackers used a stolen VPN account to gain access, said Emmanuel Jean-Georges, senior consultant with FireEye's Mandiant.

FIN5 uses a tool called GET2 Penetrator, a brute force scanning tool that looks for remote login and hard-coded credentials, as well as a free tool called EssentialNet that scans the victim's network to give the attackers "the lay of the land," Vengerik said.

RawPOS pulls information from a POS system's memory. The malware includes several components, FireEye found: Duebrew, which ensures the malware remains on the infected Windows machine, even when it gets rebooted; Fiendcry, a memory scraper that grabs the payment card data; Driftwood, which encodes the stolen payment card information to hide it from analysis tools.

Another unusual feature of FIN5's operation is that the malware code is "well-commented," Vengerik said. "That's incredibly rare in malware, the author taking time to comment on the code and to show what section of code is doing what," he said. It's like a secure development lifecycle approach, he noted.

The release notes for the Driftwood code are written in an older Russian language character set, the researchers showed.

Why would the malware author actively comment on the code? "It points to a possible ecosystem -- for advertising or support" of the malware as a product, Vengerik told *Dark Reading*.

FireEye says the attackers first target the Active Directory to get to the card data, and use tools such as Windows Credentials Editor in their quest for legit credentials. They also created several custom tools for covering their tracks and cleaning up any traces of the malware, as well as proxy tools for accessing segregated network segments.

"They also encoded hard kill-times into most of their malware for a hard end date" of the attack, he said.

Trend Micro earlier this year noted how RawPOS was able to evolve to target various types of POS software. "Aside from being multi-component, RawPOS is notable for its support for multiple PoS software. Since business establishments would have different PoS software, attackers have modified RawPOS' code to support multiple PoS software over time," Trend Micro researchers wrote in a blog post in late April.

Meanwhile, FireEye today also announced that is has partnered with Visa Inc. to power a new threat intelligence service for merchants and card issuers. The so-called Visa Threat Intelligence service is the first product under a newly forged partnership between Visa and FireEye.

"We want to offer faster, actionable intelligence to our constituents," said Mark Nelson, senior vice president of risk products at Visa.

Kelly Jackson Higgins is the Executive Editor of Dark Reading. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts
- Building a Strategy for Detection and Response
- Security Alert Fatigue: Tips for Taking Control

MORE WEBCASTS

White Papers
- Simplify Your App Security
- NetFlow vs Packet Data

MORE WHITE PAPERS

Reports
- [Report] DevSecOps & Secure App Delivery: What's Working & What's Not
- Apex Report: Global Cyber Infection

MORE REPORTS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

HOT TOPICS | EDITORS' CHOICE

Achieving DevSecOps Requires Cutting Through the Jargon 2
Mario DiNatale, Head of Platform Security. ZeroNorth, 3/19/2020

DDoS Attack Targets German Food Delivery Service 2
Dark Reading Staff 3/19/2020

Remote Workforce Jumps 15% In Two Weeks 2
Dark Reading Staff 3/17/2020

SUBSCRIBE TO NEWSLETTERS

WEBINARS

Building a Strategy for Detection and Response
Chatbots for the Enterprise
5 Steps to Integrate SAST into the DevSecOps Pipeline

WEBINAR ARCHIVES

WHITE PAPERS

- Simplify Your App Security
- NetFlow vs Packet Data
- Is Smishing the New Backdoor?
- Datacenters of the Future
- Global Application and Network Security Report

MORE WHITE PAPERS

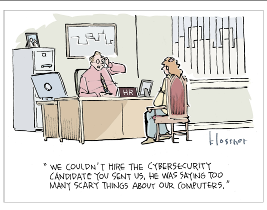
VIDEO

Ransomware Trains Its Sights on Cloud ...
7 COMMENTS

Qualys Launches Free App for IT Asset ...
1 COMMENTS

ALL VIDEOS

CARTOON



"WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

Latest Comment: Unfortunately nobody wants to spend money on security. Usually they change their mind but often it is too late

CARTOON ARCHIVE

CURRENT ISSUE

6 Emerging Cyber Threats That Enterprises Face in 2020

This Tech Digest gives an in-depth look at six emerging cyber threats that enterprises could face in 2020. Download your copy today!

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes
○ No
○ No but we are considering it
○ Still waiting for cybersecurity guidance from Trump admin EO
○ Don't know
○ Other (Please explain in the comments)

Submit

ALL POLLS

REPORTS

State of Cybersecurity Incident Response

Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents. Read this report to find out more.

DOWNLOAD NOW!

How Enterprises Are Developing and Maintaining Secure Applications — 0 COMMENTS
How Enterprises are Attacking the Cybersecurity Problem — 0 COMMENTS
How Data Breaches affect the Enterprise — 0 COMMENTS

MORE REPORTS

TWITTER FEED

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2020-5252**
  PUBLISHED: 2020-03-23
  The command-line &quot;safety&quot; package for Python has a potential security issue. There are two Python characteristics that allow malicious code to &acirc;&euro;&oelig;poison-pill&acirc;&euro;&#65533; command-line Safety package detection routines by disguising, or obfuscating, other malicious ...
- **CVE-2019-17559**
  PUBLISHED: 2020-03-23
  There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and scheme parsing. Upgrade to versions 7.1.9 and 8.0.6 or later versions.
- **CVE-2019-17565**
  PUBLISHED: 2020-03-23
  There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and chunked encoding. Upgrade to versions 7.1.9 and 8.0.6 or later versions.
- **CVE-2020-10875**
  PUBLISHED: 2020-03-23
  Motorola FX9500 devices allow remote attackers to conduct absolute path traversal attacks, as demonstrated by PL/SQL Server Pages files such as /include/viewtagdb.psp.
- **CVE-2020-10879**
  PUBLISHED: 2020-03-23
  rConfig before 3.9.5 allows injection because lib/crud/search.crud.php does not properly construct a find command.