

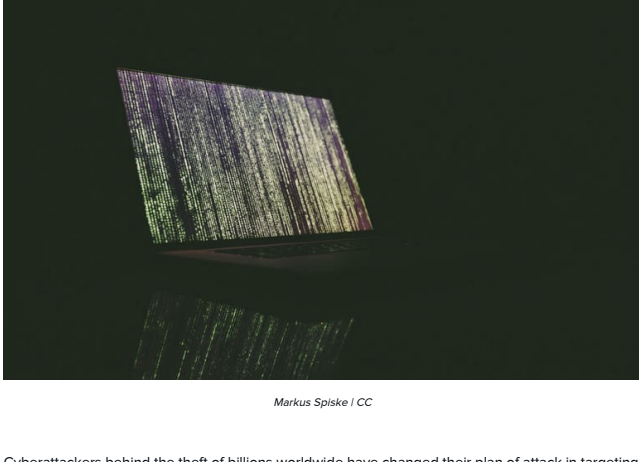
 MUST READ: [This new variant of Mirai botnet malware is targeting network-attached storage devices](#)

Carbanak hackers pivot plan of attack to target banks, the enterprise

The cyberattackers are using a fresh set of techniques to infiltrate the enterprise.



By [Charlie Osborne](#) for Zero Day | October 10, 2017 – 08:50 GMT (09:50 BST) | Topic: [Security](#)



Markus Spiske / CC

Cyberattackers behind the theft of billions worldwide have changed their plan of attack in targeting businesses across the globe.

FIN7, linked to the Carbanak Trojan, is a financially-motivated threat group which has been linked to a string of attacks against companies and financial institutions in the past.

In 2015, Kaspersky researchers uncovered the groups' involvement in the theft of **over \$1 billion** from banks over the span of two years in roughly 30 countries.

The Carbanak Trojan was at the heart of the attacks. The banks were infected through spear phishing emails and the group took advantage of poorly patched, network-misconfigured systems.

Once a system was infected, the malware provided the conduit for FIN7 to covertly spy on staff, watch how they transferred cash, and then mimic the techniques to transfer funds fraudulently without detection.

FIN7 has been connected to attacks [using legitimate software](#) which are aimed at business credentials, and recently, the hacking group has been [linked to campaigns](#) against US restaurant chains.

Cybersecurity researchers from Seattle-based [Icebrig](#) have now uncovered a change in attitude from FIN7, which has ramped up its infiltration techniques to avoid detection.

SECURITY

Windows, Ubuntu, macOS, VirtualBox fall at Pwn2Own hacking contest

COVID-19: With everyone working from home, VPN security has now become paramount

APT28 has been scanning vulnerable email servers for more than a year

Scam, spam and phishing texts: How to spot SMS fraud and stay safe

Best security keys in 2020: Hardware-based two-factor authentication for online protection

How to protect yourself from mobile malware attacks (ZDNet YouTube)

Best home security of 2020: Professional monitoring and DIY (CNET)

How to set up secure credential storage for Docker (TechRepublic)



Huawei's Wi-Fi 6 innovations are powering new enterprise networks

Customers prefer Huawei Wi-Fi 6 solutions for a number of key reasons

Sponsored by Huawei

In a blog post [earlier this week](#), researchers Alex Sirr and Spencer Walden said that FIN7 has recently focused on improving their phishing documents, with the latest update receiving a concerning initial detections on VirusTotal of 0/59 and 1/59 for RTF and DOCX formats respectively – which means that traditional antivirus software may not be enough to pick up malicious code embedded in a seemingly legitimate business email.

"While the newly observed malicious documents do not represent a "new" attack methodology, the change of payload may cause detection issues for legacy signatures and heuristic detections which utilize overly strict detection mechanisms, lacking in durability or layered coverage," the researchers said.

The threat actors use phishing to gain an initial foothold into a corporate network. Once complete, the group then paves their way through to Point of Sale (PoS) systems in order to steal credit card data, which can then be used in identity theft or potentially card cloning, should the information not be encrypted well.

FIN7 now uses a modified payload with an embedded file type for the first wave of attack. In the past, the cyberattackers have been spotted using malicious shortcut files (LNK) or visual basic scripts (VBS or VBE) to lay the trap for remote code execution.

These files were embedded into malicious documents using the Windows Object Linking and Embedding (OLE) framework.

However, it appears the hackers are now switching from LNK files to OLE embedded CMD files. These files are underlain with JScript, and writes a "txt.txt" files to the victim's home directory. The script then uses the JScript engine on the file, also leading to code execution, but is more difficult to spot.

In addition, FIN7's custom backdoor, HALFBAKED, has evolved. In the newest version, changes have been made to obfuscation techniques.

Originally, HALFBAKED utilized base64 encoding, stored in a string array variable called "srcTxt." Now, this name is obfuscated and the string is broken up into multiple strings.

The backdoor is also equipped with a command called "getNK2" which is designed to covertly pull a victim's full Microsoft Outlook email client auto-complete list, which suggests the threat group is keen to acquire as many new targets as possible.

"Detection authors must make trade-offs to optimize signature performance; narrow signatures lead to high fidelity detections, but risk missing changes in actor behaviors, meanwhile broader detection patterns provide better coverage, at the risk of more false positives," the researchers note. "Combating a well-resourced and adaptive adversary requires a layered approach of both signature styles."

Must-have mobile apps to encrypt your texts...

SEE FULL GALLERY



1 - 5 of 9

NEXT >

PREVIOUS AND RELATED COVERAGE

[Cybercrime gang uses Google services for malware command and control](#)

Gang behind multiple cyberattacks on banks and financial institutions has found a new way to manage its activities.

[Carbanak hacking group steal \\$1 billion from banks worldwide](#)

Carbanak malware offered criminals the chance to steal up to \$10 million per heist.

[New Trojan malware attack targets restaurant chains](#)

Dubbed Bateleur, this malware uses with macro-laden phishing emails that allow attackers to take screenshots, steal passwords, and more.

RELATED TOPICS:

SECURITY TV

DATA MANAGEMENT

CSX

DATA CENTERS



By [Charlie Osborne](#) for Zero Day | October 10, 2017 – 08:50 GMT (09:50 BST) | Topic: [Security](#)

Recommended For You



New Classy \$109 Smartwatch Takes Italy By Storm
Smart Watch



Verona: Le auto che nel 2019 sono rimaste invendute non dovrebbero...



Se hai più di 50 anni, questo gioco è un must! Vikings: Giochi online gratuiti



Prezzi Luce a partire da 0.076 kWh. Confrontati tutti quelli



Il costo dell'assicurazione auto a Verona potrebbe sorprenderti



Il gioco di strategia più coinvolgente del 2020 Total Battle: Giochi di Strategia Online

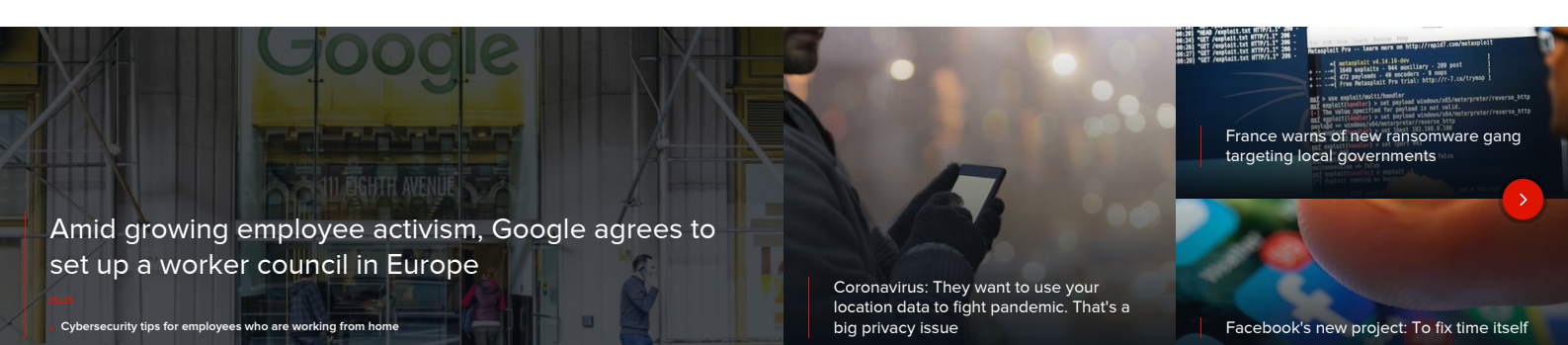


A browser che's 200% Faster than Chrome Browserguides.com for Brave



Sugar creamosa. 1 55% di zuccheri in

SHOW COMMENTS



Amid growing employee activism, Google agrees to set up a worker council in Europe

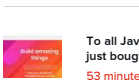
Cybersecurity tips for employees who are working from home

Coronavirus: They want to use your location data to fight pandemic. That's a big privacy issue

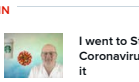
France warns of new ransomware gang targeting local governments

Facebook's new project: To fix time itself

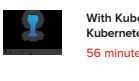
JUST IN



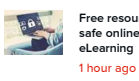
To all JavaScript developers: Microsoft just bought npm
53 minutes ago



I went to Starbucks, saw the post-Coronavirus future, and really didn't like it
56 minutes ago



With Kubecf, Cloud Foundry comes to Kubernetes
56 minutes ago



Free resource to help parents keep kids safe online as schools move to eLearning
1 hour ago

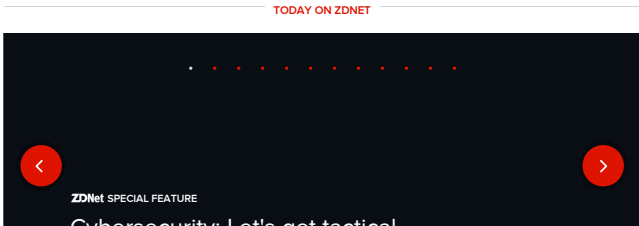
The smartphone still has a shapeshifting future
2 hours ago

Celebrity influencers on the wane: Most brands will choose micro-influencers in 2020
2 hours ago

Coronavirus tech conference cancellations list: Apple WWDC, Microsoft Build, E3, NAB, Gartner, Dell World and more
2 hours ago

Hackers breach FSB contractor and leak details about IoT hacking project
2 hours ago

TODAY ON ZDNET



Using Slack a lot lately? It just revamped its user interface

Slack said the update marks the biggest change to its user interface since the platform launched seven years ago.
3 hours ago by ZDNet Editors in Collaboration

Data science vs the COVID-19 pandemic: Flattening the curve -- but how?

Whether they are epidemiologists or not, a few people have attempted to use data and predictive models to model the COVID-19 pandemic. Let's look at the models, the data, and the assumptions and implications that come with them.
4 hours ago by George Anadiotis in Data Management

AWS commits \$20 million to speeding up COVID-19 diagnostic development

The effort is designed to bolster collaboration between customers and be funded with AWS in-kind credits and technical support.
4 hours ago by Larry Dignan in Cloud

AT&T cancels \$4 billion share repurchase due to coronavirus uncertainty

The company will instead use the funds to pay employees and make network investments.
5 hours ago by Natalie Gagliardi in 5G

BT removes data caps on home broadband as companies move to remote working

Unlimited data for customers as workers increase the load on home broadband.
5 hours ago by Steve Ranger in Networking



Microsoft: PowerShell's new 'secrets' tool preview is out

Microsoft Secrets Management module is for managing secrets in heterogeneous clouds.
5 hours ago by Liam Tung in Enterprise Software



Email/Instant Message/Voicemail Retention policy

Maintaining electronic communications in business involves walking a fine line. Employees want relevant information to be kept available for future reference so that they can do their jobs, but keeping...
from TechRepublic Premium

A professor says Edge is the worst for privacy. Microsoft isn't happy

Could it be that Google was right to accuse Microsoft Edge of being insecure? New research suggested it's the least private browser you can have. So I asked Redmond what it thought.
5 hours ago by Chris Matyszczyk in Microsoft

Ransomware: How hackers are evolving attacks, and how to protect yourself

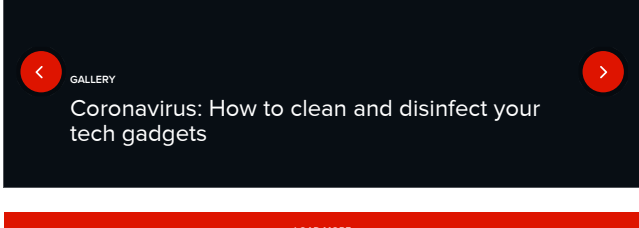
ZDNet Security Update: Danny Palmer talks to Sherrod DeGrip, senior director of threat research and detection at Proofpoint, about the latest trends in ransomware.
6 hours ago by Danny Palmer in Security

WHO chief emails claiming to offer coronavirus drug advice plant keyloggers on your PC

Fraudsters are trying to capitalize on fears surrounding the illness in new phishing campaigns.
6 hours ago by Charlie Osborne in Security

Programming languages: Python and Java VS Code extensions get these new updates

Java for Visual Studio Code now gets SolarLint 'spellchecker' tool, while the Python extension gets a new debugger.
6 hours ago by Liam Tung in Enterprise Software



LOAD MORE

Recommended For You

Sponsored Links by Taboola



Come guadagnare 9.000€ al mese con Amazon



Le migliori VPN del 2019



How To Get Unrestricted Internet Access Worldwide With One Simple Tool



Scopri i migliori fornitori luce e gas del 2019, da scegliere per il 2020.

NEWSLETTERS

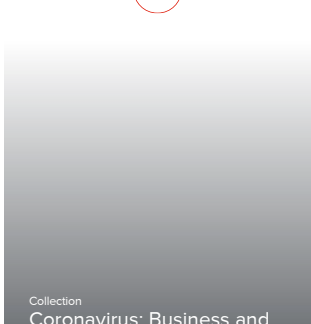
ZDNet Announce UK

ZDNet's Announcements newsletter offers a mix of stories, special offers and members-only benefits.

Your email address

SUBSCRIBE

SEE ALL



To all JavaScript developers: Microsoft just bought npm

I went to Starbucks, saw the post-Coronavirus future, and really didn't like it

Using Slack a lot lately? It just revamped its user interface

Ransomware: How hackers are evolving attacks, and how to protect yourself

Incorporating prescription lenses into smart glasses

IT skills: How investment into the UK tech industry is booming



Wyndham Hotels & Resorts tackled technical debt: cloud, hybrid cloud in a hurry (Cloud TV)

HSBC charts out its move to the cloud (Cloud TV)

How Brinker International thinks through cloud, data, Apple iPads (Cloud TV)

Why security is the top barrier in enterprise cloud adoption (Hybrid Cloud TV)

How New Belgium Brewing evaluated managed vs. private cloud (Hybrid Cloud TV)

With Red Hat, IBM to become the leading hybrid cloud provider



CONNECT WITH US



Topics

About ZDNet

Join / Log In

Galleries

Meet The Team

Membership

Videos

All Authors

Newsletters

Sponsored Narratives

RSS Feeds

Site Assistance

CA Privacy/Info We Collect

Site Map

ZDNet Academy

CA Do Not Sell My Info

Reprint Policy

TechRepublic Forums

Manage Cookies