




HOME	ISBUZZ-JOBS	PARTNERSHIP ENQUIRIES	FREE RESOURCES	TRAINING
EVENTS & CONFERENCES		DIRECTORY		



Connecting InfoSec
with News

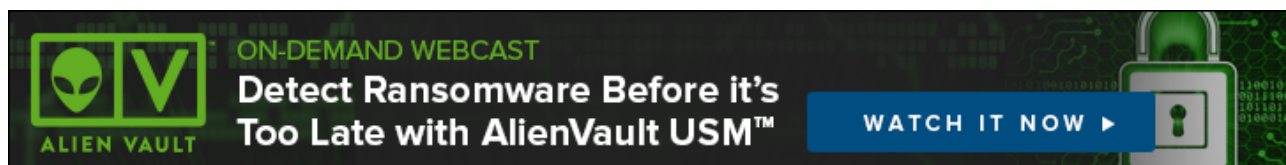
NEWS	HACKER NEWS	SECURITY ARTICLES	STUDY	HOW TO	EXPERT PANEL
SECURITY VIDEOS		SECURITY EDUCATION			

HOME » HACKERS USING SOCIAL MEDIA TO EXECUTE ATTACKS

Hackers Using Social Media to Execute Attacks

F-Secure On December 18, 2015 — [Leave A Comment](#)

F-Secure researcher authors new report exploring how hackers are using third party services to spread malware and extract stolen data from victims.



A researcher from [F-Secure Labs](#) has written a [new report](#) examining how hackers use third party services to coordinate malware campaigns. The paper was published by Virus Bulletin for its VB2015 conference and examines how the [encryption](#) used by online services like Twitter enable attackers, such as the state-sponsored group The Dukes, to spread malware and steal data.

"If I had to put it in a nutshell, I'd say that attackers are using certain third party services to help them fly under the radar of corporate security," said **F-Secure** Researcher **Artturi Lehtiö**, who authored the report and presented his findings at VB2015. "Many online services use

encryption to prevent data from being intercepted and stolen while in transit, but the downside of this is that security measures like firewalls aren't able to identify malicious traffic. It's a real challenge for companies, and my research has shown how attackers like The Dukes capitalise on this advantage in their attacks."

The Dukes are a group of state-sponsored attackers that have been targeting governments and related organisations for at least the last seven years and were the topic of a recent whitepaper published by F-Secure Labs. Lehtiö's new report provides details on how The Dukes execute attacks by using third party services as what security researchers call "command and control" infrastructure – essentially a tool to coordinate attacks.

The report specifically highlights how The Dukes were able to use Twitter to communicate with infected machines and direct them to download additional malware. The Dukes were also able to use Microsoft OneDrive as a data exfiltration tool, allowing them to retrieve stolen data without drawing attention to themselves.

"Using these services as command and control infrastructure lets attackers piggyback on the network access given to reliable online platforms," said **Lehtiö**. "Attackers use them for communication with devices that they've already infected so, in these cases, they're not being used to directly target the service providers or random users. Things like social media simply give attackers a user-friendly, cost effective tool to coordinate their campaigns to make sure they achieve their objectives."

Malware campaigns using third party services are often difficult for companies to detect because the malicious data exchanged between attackers and their targets is encrypted and mixed together with legitimate traffic. Research suggests that many companies are not actively decrypting web traffic to differentiate between the two. One study found that less than fifty per cent of companies with dedicated secure web gateways decrypt outbound traffic, and less than twenty percent of organisations with firewalls, intrusion prevention systems or unified threat management appliances decrypt inbound or outbound SSL traffic.

But according to **F-Secure** Senior Researcher **Jarno Niemelä**, relying on security solutions that decrypt Internet traffic can be a risky proposition and companies need to be aware of the potential difficulties in this approach. "Decrypting network traffic using man-in-the-middle techniques can be costly and very complicated to do properly. There have been cases where attackers have taken advantage of this approach to access their victim's encrypted Internet traffic, essentially exposing confidential information rather than securing it. Companies taking this approach should make sure they have a unique certificate given only to their organisation, as using shared certificates greatly increases the risk of a man-in-the-middle attack."

Niemelä added that reliable **endpoint protection** can disrupt these attacks at the point of the initial infection as it does not depend on being able to break or bypass encryption, making it a safe, efficient way for companies to protect themselves. Both of F-Secure's corporate security

offerings, [Business Suite](#) and [Protection Service for Business](#), use award-winning endpoint protection technology to detect and prevent malware infections.

About F-Secure



F-Secure was founded in Helsinki, Finland in 1988. There were just a few of us back then – a few passionate people who cared deeply about doing things right. A lot has changed in all those years. The digital world grew up, and so did we. But although we're now a world leader in security, we've never lost the values we were established on – privacy, integrity, transparency and trustworthiness. The battles have changed through the years. Malware and other online threats evolve, but the fight remains the same.



Beginners Guide to SIEM

[DOWNLOAD FREE GUIDE ►](#)

Shares

Please Share:



submit

[Tweet](#)

[G+1](#)

0

[Pinterest](#)

[tumblr.](#)

[in Share](#)

1

[f Share](#)

1

[More](#)

G+

Related

in

1

f

1



Annual Threat Report Sheds Light on Emerging Security Risks In "Research"



Starwood POS Data Breach In "Hacker News"



Cyberattacks Linked to Russian Intelligence Gathering In "Security Articles"

Banking Malware Targets



Comments on new PCI DSS Standard Security Articles"

Want to join the best information security community in the world?

Become a Information Security Buzz member and join thousands of infosec professionals who receive our weekly newsletter that will provide you with offers, discounts and our best blogs.

Enter your Email

CRYPTING

Enter your Email

JOIN NOW

Powered by SumoMe

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

POST COMMENT

☐ Notify me of followup comments via e-mail. You can also [subscribe](#) without commenting.

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

**HOT CYBER
SECURITY JOBS**

>

Cyber Security Architect

>

IT Forensic Investigator

>

FSS Security CISO Advisor

>

Cybersecruity Attorney



ALIEN VAULT

ON-DEMAND WEBCAST

**Detect Ransomware
Before it's Too Late
with AlienVault USM™**



WATCH IT NOW ▶

POPULAR


LATEST

TODAY


WEEK

MONTH


ALL




> What Nefarious Cyber-Acts will Define 2016?




> A Brief History of Ransomware



> The Internet of Toys



> 6 Technology Predictions for 2016



> Machine Learning is Cybersecurity's Latest Pipe Dream



Tweets

**Info Security Buzz**

26m

@Info_Sec_Buzz

Over 30 per cent of companies use mobile devices to access corporate bank accounts:

informationsecuritybuzz.com/study/survey/e...

@kaspersky #cyberbullying #iot

Expand

**Info Security Buzz**

1h

@Info_Sec_Buzz

Microsoft Office 365 to relieve the growing headache of managing security in-house.:

informationsecuritybuzz.com/articles/secur...

@databarracks #cyberthreat

Expand

**Info Security Buzz**

1h

@Info_Sec_Buzz

What Nefarious Cyber-Acts will Define 2016? -

informationsecuritybuzz.com/articles/what-...

pic.twitter.com/BHu3ZqS5cW



Get All The Latest News
By Email

Subscribe Today!

OK

FBF ■ Powered by @Google Feedburner

Sign Up To Our Newsletter!**SIGN UP****WELCOME TO
INFORMATION
SECURITY BUZZ**

Information Security Buzz is an independent resource that provides the best blogs, opinions and news for the information security community. Collated from security experts and industry leaders, content is carefully selected to provide you with the latest threat trends, insights, practical solutions, hot topics and advice from around the globe.

RESOURCES**ADVERTISERS**[Media Pack](#)**USER CENTRE**[About Us](#)[Contact Us](#)[Article Submission](#)**RETURN TO TOP**

Copyright © 2015 Informationsecuritybuzz.com All Rights Reserved