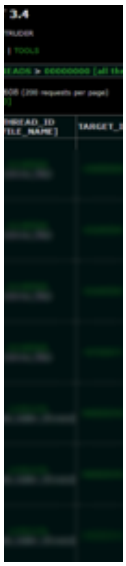
MUST READ Espionage campaign relying on the Zeus Trojan targets the Israeli Public

FIN5 hacking crew steals 150,000 credit cards from casino

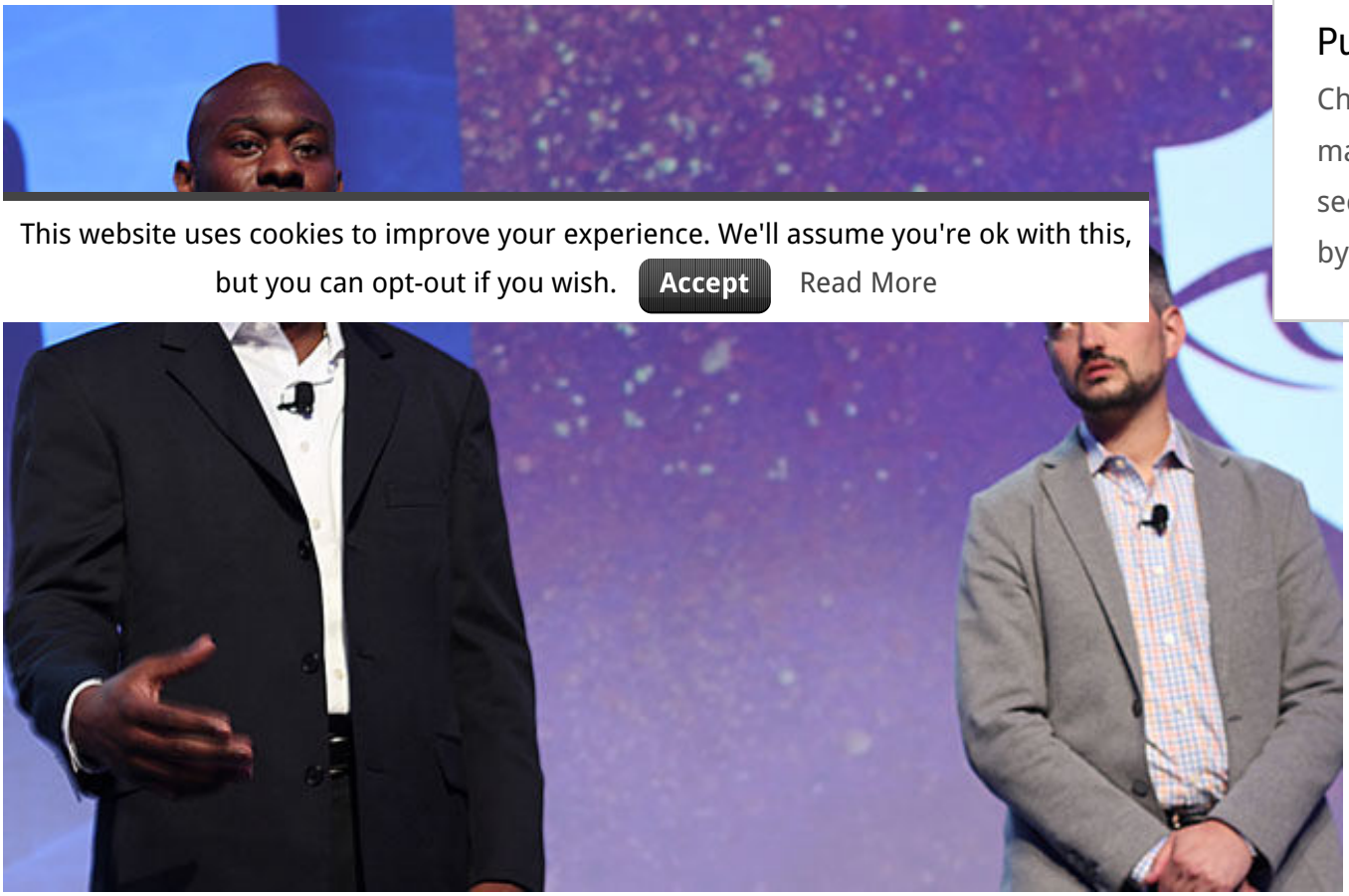
October 14, 2015 By Pierluigi Paganini

FireEye has uncovered a new hacking group dubbed FIN5 hacke payment systems of an un-named Casino and it has stolen near 150,000 credit cards.

The fact that the game can create problems is not a novelty, news of the day is that an un-name Casino has lost 150,000 credit cards. The cause of the data breach also in this case is a cyber att



According to the researchers Emmanuel Jean-Georges and Barry Vengerik of Mandiant and Fire the hacking crew behind the attack is the "Fin5."



The Fin5 is linked to numerous payment card breaches including Goodwill, the hacking group is also known for the use of the "RawPOS" malware that allowed the gang to raid payment systems worldwide by scraping the memory of PoS searching for credit card data.

RAWPOS malware is a memory scraper that has infected lodging merchants since 2008 by targeting the memory dump where payment information may be temporarily stored, and that data are staged on a network and removed later by a separate process.

Fin5 is prolific and long-running cybercrime ring that has been the subject of multiple Visa security alerts to merchants due to the use of its malware.

"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." *states* FireEye .

How the hackers raided the payment systems at the Casino?

Experts at FireEye/Mandiant confirmed the poor security implemented by the IT staff of the Casino, its payment platforms were not protected by network appliance, neither by strong authentication mechanisms.

The hackers at FIN5 group hack organizations by using stolen credentials, then they target Active Directory to obtain more credentials and gain lateral movement.

"It is classic lateral compromise," Vengerik says. "It was a very flat network, single domain, with very limited access controls for access to payment systems," explained Emmanuel Jean-Georges during the Cyber Defence Summit (formerly Mircon) in Washington DC. "Had this casino hotel operator had even minimal or basic protections in place like a firewall with default deny systems to limit access to PCI (payment) systems … it would have slowed down the attackers and hopefully set off red flags."

Unfortunately, the casino isn't the unique organization hit by the hackers, FireEye has identified at least another six card breach.

Vengerik explained that the threat actors have targeted at least two payment systems providers and in cascade their customers, the un-named casino is one of them.

In the specific attack against the Casino, the experts discovered that the Fin5 gang used a backdoor codenamed Tornhull and a VPN dubbed Flipside to maintain the control over the compromised system.

In the arsenal of the FIN5 group there was also a tool called GET2 Penetrator, which is a brute force scanning tool that search for remote login and hard-coded credentials, and a free tool called EssentialNet that is used to scan the target network.

The RawPOS malware includes several components such as the Duebrew, which is used to maintain persistence on Windows machines, the memory scraper Fiendcry and Driftwood used to encode the stolen payment card information.

Stay Tuned!.

Pierluigi Paganini

(Security Affairs – Fin5, credit card)

credit card | Cybercrime | Fin5 | FireEye | Hacking | malware | ROWPOS

Breaking News | Cyber Crime | Malware

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Espionage campaign relying on the Zeus Trojan targets the Israeli Public Sector

NEXT ARTICLE
Google records and maintains all our voice searches

YOU MIGHT ALSO LIKE

Pangu cracking team has released the iOS 9 jailbreak

October 14, 2015 By Pierluigi Paganini

Espionage campaign relying on the Zeus Trojan targets the Israeli Public Sector

October 14, 2015 By Pierluigi Paganini