PwC Weekly Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

Malware

'Invisible' memory-based malware hit over 140 banks, telecoms and government agencies

Data breach

Debit card breach: Malware compromised our systems, says Hitachi Payment Services

Data breach

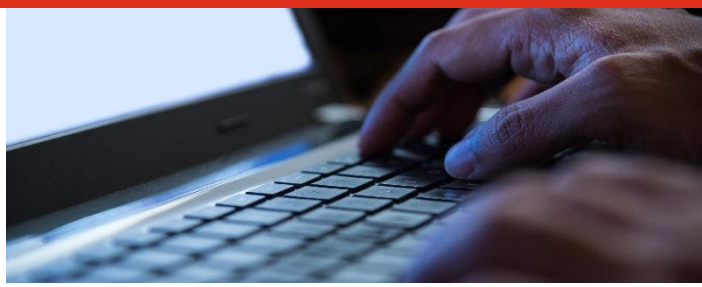
Arby's confirms security breach that saw hackers steal credit card data of thousands of customers

Top story

Microsoft just beefed up Windows and Office 365 enterprise security features

pwc

'Invisible' memory-based malware hit over 140 banks, telecoms and government agencies



Anti-forensic techniques such as the malware vanishing after reboot makes attribution nearly impossible.

Cybercriminals have hit more than 40 countries with hidden malware that steals passwords and financial data. The malware is not found on hard drives as it hides in the memory of compromised computers, making it almost "invisible" as criminals exfiltrate system administrators' credentials and other sensitive data. When a targeted machine is rebooted, nearly all traces of the malware disappear.

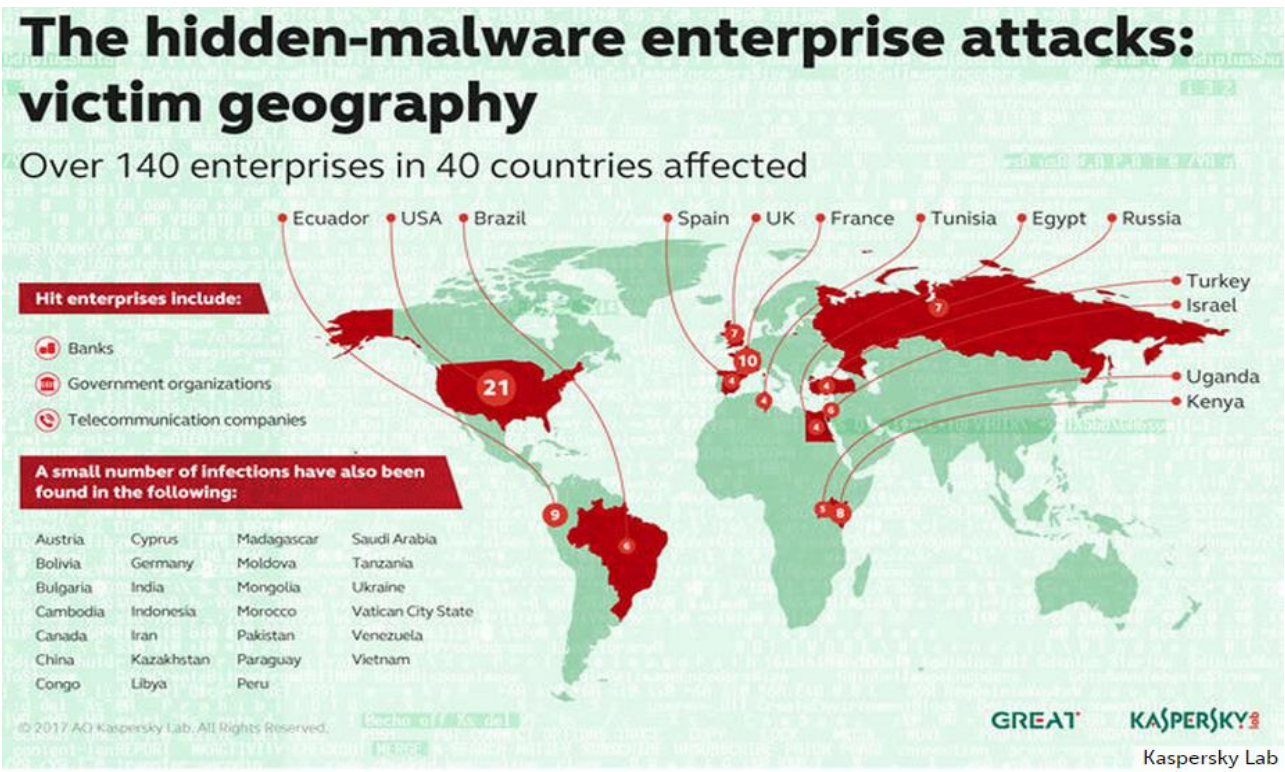
Over 140 enterprise networks – banks, government organizations and telecommunication companies – from 40 countries have been hit, according to Kaspersky Lab. The cybercriminals are using methods and sophisticated malware previously used by nation-state attackers.

The U.S. has been the most targeted country with 21 hidden-malware attacks, followed by 10 attacks in France, nine in Ecuador, eight in Kenya, and seven in both the UK and Russia.

Because the malware manages to hide so well, and poofs after a reboot, the number of infections may be much higher.

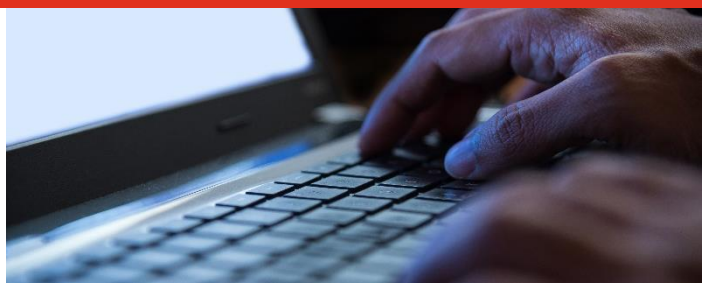
The "attacks are ongoing globally against banks themselves," Kaspersky Lab's Kurt Baumgartner told Ars Technica. "The banks have not been adequately prepared in many cases to deal with this." The attackers are "targeting computers that run automatic teller machines" in order to push "money out of the banks from within the banks."

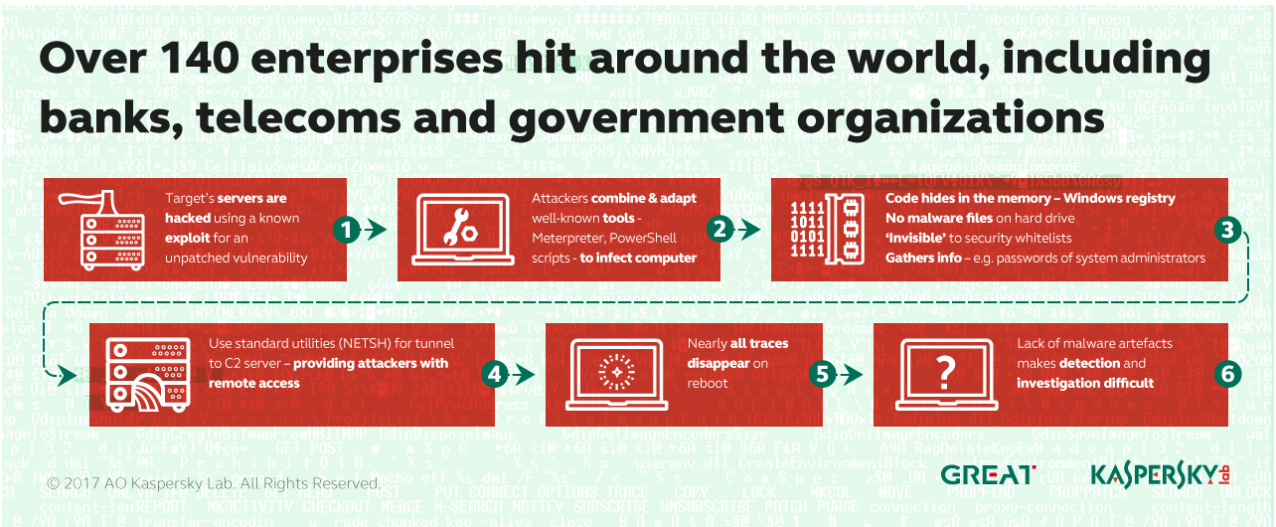
The attackers have embraced anti-forensic techniques to avoid detection; malware loaded to RAM instead of a hard drive helps to keep it undetected as data is being stolen and systems are being remotely controlled. The attackers have used expired domains that have no WHOIS information. By using open source and legitimate tools, the cybercriminals are making attribution nearly impossible.



Kaspersky Lab

'Invisible' memory-based malware hit over 140 banks, telecoms and government agencies





Researchers from Kaspersky Lab first learned of the "fileless" malware after a bank was attacked and it helped with forensic analysis. The bank found Meterpreter code in the memory of a server; Meterpreter was not supposed to be in the physical memory of the domain controller. Digging deeper, the researchers learned that the code had been injected into memory using PowerShell commands. The PowerShell scripts were hidden within Windows registry.

The attackers used Mimikatz, Kaspersky Lab said, to grab credentials from accounts with administrative privileges and NETSH to send stolen data back to their server.

It is presently unclear if the attacker is one group or if several groups are using the same tools. "Given that the attackers used the Metasploit framework, standard Windows utilities and unknown domains with no WHOIS information, this makes attribution almost impossible," wrote Kaspersky Lab. However, the researchers noted that similar techniques have been used by the groups GCMAN and Carbanak.

Kaspersky Lab will reveal more details about the attack, as well as how the cybercriminals withdrew money from ATMs, at its Security Analyst Summit in April.

For now, Kaspersky has listed indicators of compromise; "detection of this attack would be possible in RAM, network and registry only." After an infected machine is cleaned, all passwords must be changed. "This attack shows how no malware samples are needed for successful exfiltration of a network and how standard and open source utilities make attribution almost impossible."

Source:
http://www.computerworld.com/article/3167533/security/invisible-memory-based-malware-hit-over-140-banks-telecoms-and-government-agencies.html

Debit card breach: Malware compromised our systems, says Hitachi Payment Services

The data breach in India's banking system, which affected nearly 32 lakh debit cards in 2016 was caused by a security compromise at Hitachi Payment Services' systems, the company said on Thursday. In a statement, Hitachi said a malware injection in mid-2016 caused the breach in its systems and that the malicious software was able to "work undetected" while trying to make itself untraceable, Mint reported.

The company also said that it could not determine how much data had been compromised by the malware. "Hitachi Payment Services regrets the inconvenience caused to banks and its customers due to this lapse in its security infrastructure," the company's Managing Director Loney Anthony said.

Hitachi's acknowledgement came a day after information security specialist SISA Information Security Private Limited completed an audit of the company's systems, Business Standard reported. SISA confirmed that the malware captured the debit card numbers and PINs of customers who used their cards at ATMs affected by it. However, banks managed to contain losses by blocking the cards affected and advising their customers to change their PINs.

"The reason why such cyber attacks are happening today is because of the ineffective implementation of the payment security standards," SISA Chief Executive Officer D Shanthamurthy said. "With demonetisation, and with an increase in the number of digital payments, such attacks are going to get worse," he added.

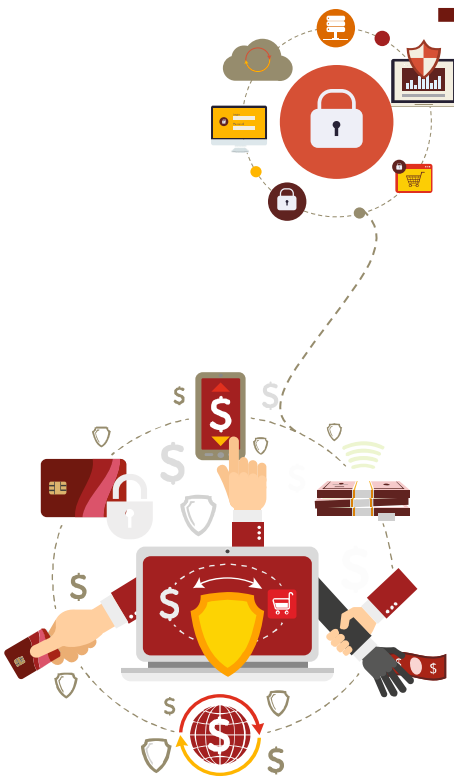
Nineteen banks and 641 customers had complained of fraudulent withdrawals amounting to Rs 1.3 crore, the National Payments Corporation of India had said on October 21, 2016. At least 32 lakh debit cards were compromised because of the breach, which was first reported only after several customers complained to banks that their cards had been used in China at various ATMs and point of sale terminals. The Centre had said that it would take action against the perpetrators.

The malware, which overwrites the master boot record of a computer, rendering it inoperable, has already destroyed thousands of computers across multiple government agencies, two people familiar with the probe said.

Source:
https://scroll.in/latest/829004/debit-card-breach-malware-compromised-our-systems-says-hitachi-payment-services

Our perspective

As Hitachi Systems have confirmed that their payment system was compromised and affected by malware, card users are advised to periodically change their card PIN to avoid any leakage. They are also advised to check for any irregular transactions periodically and inform their bank about any irregularities they find.



Arby's confirms security breach that saw hackers steal credit card data of thousands of customers

American fast food chain Arby's has reportedly confirmed that it was hit by hackers in a massive data breach that is believed to have affected thousands of customers. The hackers infected the fast food chain's payment card systems with malware at hundreds of its restaurants across the US, according to reports.

Arby's claimed that it was alerted about the breach in mid-January, but refrained from informing its customers about the breach at the FBI's request, cybersecurity journalist Brian Krebs reported in his blog.

"Arby's Restaurant Group, Inc (ARG) was recently provided with information that prompted it to launch an investigation of its payment card systems," the company said in a statement. "Upon learning of the incident, ARG immediately notified law enforcement and enlisted the expertise of leading security experts, including Mandiant. While the investigation is ongoing, ARG quickly took measures to contain this incident and eradicate the malware from systems at restaurants that were impacted."

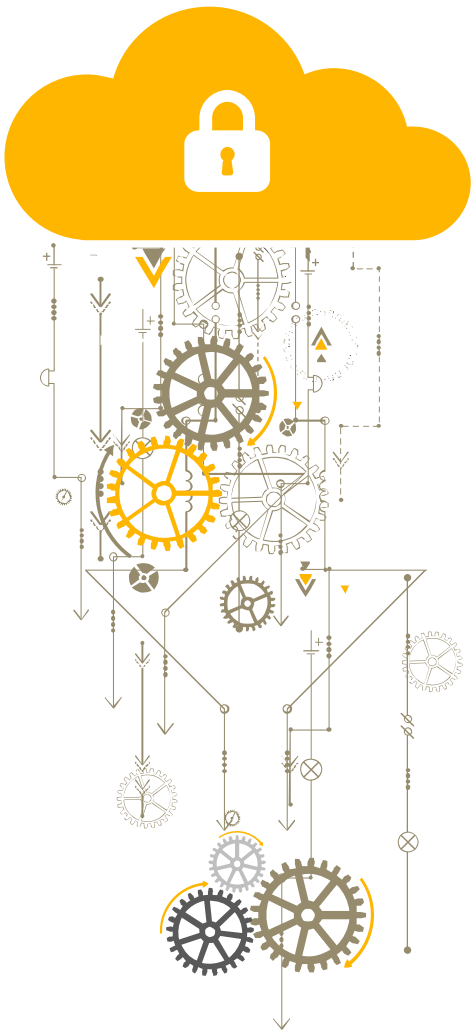
Arby's claimed that the malware infected payment systems within its corporate stores, adding that Arby's franchised restaurant locations were not affected.

"Although there are over 1,000 corporate Arby's restaurants, not all of the corporate restaurants were affected," said Christopher Fuller, Arby's senior vice president of communications. "But this is the most important point: That we have fully contained and eradicated the malware that was on our point-of-sale systems."

According to the credit union service PSCU, which first alerted member banks about a long list of compromised Visa and MasterCard numbers, over 355,000 credit and debit card accounts may have been impacted by the hack.

Arby's is not the first American fast food chain to be the victim of a massive cyberattack. In 2016, burger chain Wendy's disclosed that cybercriminals hacked hundreds of its restaurants in a massive targeting payment card data. It appears that 2016's data breach trend may be spilling over into 2017 as well.

Source:
http://www.ibtimes.co.uk/arbys-confirms-security-breach-that-saw-hackers-steal-credit-card-data-thousands-customers-1605862



Microsoft just beefed up Windows and Office 365 enterprise security features

Microsoft has just helped IT professionals around the world breathe a bit easier. As a lead up to the RSA Security Conference, the software giant has announced a wide variety of new security features aimed at enterprise administrators. The new tools for Windows and Office 365 will help better manage devices and beef up their cyber security.

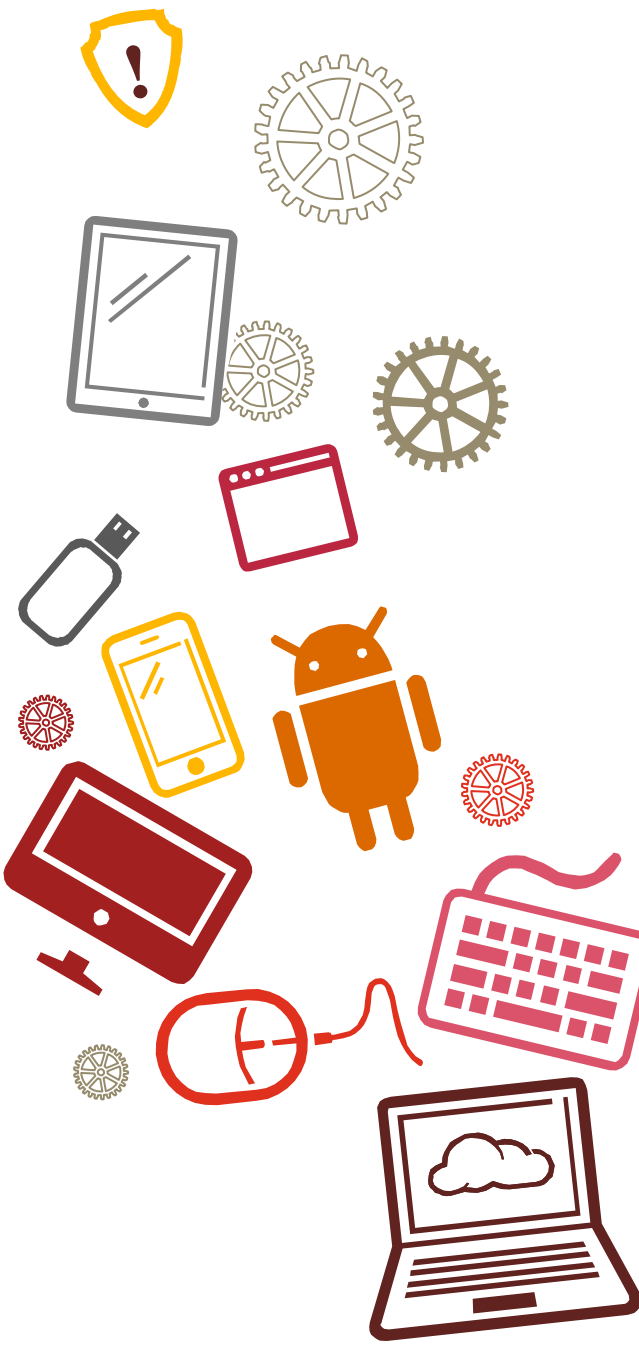
The biometric authentication system Windows Hello will be getting two new upgrades in the Windows 10 Creators Update. The service will now be compatible with standard on-site Active Directory systems instead of requiring the cloud based Azure Active Directory. For devices with Bluetooth connectivity, a new auto-locking feature will be available. Users can pair their phone and computer and once they leave their desk and walk out of range, the computer will lock itself. This is very similar to Android's trusted device feature.

Surface devices will get a new Enterprise Management Mode which will enforce hardware level restrictions like disabling the microphone or network connectivity. It works at the UEFI level so most traditional hacks can't penetrate it. There will also be tighter integration between Group Policy and mobile device management (MDM) software to allow administrators to more easily manage their devices.

Office 365 will be receiving a new automatic security audit tool for organizations. It will analyze how well the organization has deployed the available security features and then give them a rating. Users can also see what other security settings are available to implement and the impact they would have.

In addition, a private beta will be starting soon for the Office 365 Threat Intelligence service. It will give administrators in-depth analysis of threats affecting their network and other emerging threats around the world.

Source:
http://www.in.techspot.com/news/security/microsoft-just-beefed-up-windows-and-office-365-enterprise-security-features/articleshow/57100076.cms



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,23,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

AW/February2017-8756