Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE*

Audience: Acquirer/Issuer/Processor/Merchant/Service Provider
Category: Technical (IT, Information Security)

Visa recently identified an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane or on Back-of-the-House (BOH) servers to extract full magnetic stripe data in random access memory (RAM).

Point-of-sale (POS) malware has been designed to remove unencrypted card data from the memory of an unprotected device. To combat this type of attack, either encrypt card data at a secure reading and exchange of data (SRED) device or apply strict PCI DSS controls to the POS computer. Examples of appropriate controls are described below.

Visa is issuing this alert to make clients aware of new malware information and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access. Visa highly recommends merchants implement these signatures on security solutions to detect a suspected breach. However, Visa recommends performing sufficient due diligence prior to implementing any block to avoid any inadvertent connectivity issues for legitimate access.

At the present time, Visa is only aware of the malware impacting a Windows operating system.

Recommended Mitigation Strategy

These strategies are broken down into five categories 1) Network Security; 2) Point of Sale (POS); 3) Administrator Access; 4) Incident Response; and 5) Third Party Management to ensure a defense-in-depth approach to minimize the possibility of an attack and mitigate the risk of a card data compromise:

1) Network Security

- Review your firewall configuration and ensure only allowed ports, services and IP (internet protocol) addresses are communicating with your network. This is especially critical on outbound (e.g., egress) firewall rules, where compromised entities allow ports to communicate to any IP on the Internet. Hackers will leverage this misconfiguration to exfiltrate data to their IP address.
- Segregate the payment processing network from other non-payment processing networks.
- Apply access controls lists (ACLs) on the router configuration to limit unauthorized traffic to the payment processing networks.
- Create strict ACLs segmenting public facing systems and backend database systems that house payment card data.
- Review systems that have direct connectivity or access to the payment processing environment and ensure systems are secure.

2) Cash Register and POS Security

- Implement hardware-based point-to-point encryption. Visa recommends EMV enabled PIN Entry Devices or other credit only accepting devices that have Secure Reading and Exchange of Data (SRED) capabilities. SRED approved devices can be found on www.pcisecuritystandards.org.
- Install PA-DSS compliant payment applications and ensure applications are installed in a PCI DSS compliant manner. Merchants should also review their payment application to ensure it is not configured in a debug/troubleshooting mode. This type of configuration can result in storage of clear-text cardholder data.
- Perform periodic scans on systems to identify storage of cardholder data and secure delete the data.
- Deploy the latest version of operating system and ensure it is up-to-date with security patches, anti-virus software, File Integrity Monitoring, and a host-based intrusion detection system.
- Assign strong passwords to your security solution to prevent application modification.
- Perform a binary or checksum comparison to ensure unauthorized files are not installed on systems. Merchants should consider implementing application "whitelisting" to help prevent installation of malicious software and other unapproved programs from running.
- Deny Remote Desktop Protocol (RDP) logons whenever possible.

- Ensure any automatic updates from third-parties are validated. This means performing a checksum on the updates prior to deploying on the POS systems. Merchants should work with their POS vendors to obtain signatures/hash values in order to perform this checksum validation.
- Disable unnecessary ports and services, null sessions, default users and guests.
- Enable logging of events and confirm you have a process to monitor logs on a daily basis.
- Implement least privileges and ACLs on users and applications on the system.

Note that the malware/memory parsers used in attacks against retail POS systems are also believed to have the capability to obtain data from an automated teller machine (ATM) terminal memory. To protect ATMs against these types of attacks, Visa recommends following the Payment Card Industry Security Standard Council's *ATM Security Guidelines* (https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf).

3) Limit Administrative Access

- Use two-factor authentication when accessing the payment processing networks. Even if a Virtual Private Networking (VPN) is used, it is important that 2-factor authentication be implemented. This will help to mitigate key logger or credential dumping type of attacks.
- Limit administrative privileges on users and applications.
- Periodically review systems (local and domain controllers) for unknown and dormant users.
- Do not use NTLM or LM hash for password hashing as the algorithm is known to be compromised and susceptible to a Pass-the-Hash type of attack. Visa recommends implementing salted one way password hashing. For more information on Pass-the-Hash attacks and additional password mitigation controls, go to http://www.microsoft.com/security/sir/strategy/default.aspx#!password_hashes.

4) Incident Response

- Deploy Security Information and Event Management (SIEM). A SIEM is a system that serves as a central point for managing and analyzing events from network devices. A SIEM has two primary responsibilities:

    1. Aggregate events and logs from network devices and applications
    2. Use intelligence to analyze and uncover malicious behavior on the network

- Since anti-forensic techniques are used by hackers to avoid detection, Visa recommends offloading logs to a dedicated server in a secure location to prevent unauthorized users from tampering with the logs.
- Invest in a dedicated incident response team (IRT). The IRT should have the knowledge, training and certification to respond to a breach. For more information on IRT training, go to www.sans.org.
- Test and document your incident response plan to identify and remediate any gaps in the process prior to an actual event. The plan should be tested and updated periodically to address emerging threats.

5) Third Party Management

- Avoid providing unrestricted access or remote maintenance capability to third party vendors – specifically to your production environment.
- Establish a vendor demilitarized zone (DMZ) zone, sometimes referred to as a perimeter network.
- Ensure adequate review of third party vendors' security practices in the event they will handle sensitive data on your behalf.
- Obtain information about the vendor's "partner" operations to understand how it may impact your business.

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com

- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For more information, please contact Visa Risk Management or cisp@visa.com

APPENDIX A

Malware Signatures	Filename	MD5 Hash Value
	svchosts.exe	ce0296e2d77ec3bb112e270fc260f274
	svchosts.exe	ce0296e2d77ec3bb112e270fc260f274
	svchosts.exe	f7c20a277929c4cb70999aff1b03388e
	2wce.exe	93405c57e915680f0182650fb75c47ee
	DUMPSEC.exe	65dd8d2d9604d43a0ebd105024f09264
	ftprmt.exe	abb234773b0ad268f9a554c7ee597489
	ftprt.exe	4352e635046aa624dff59084d5619e82
	getlsasrvaddr.exe	0b33b4d61ea345f16c4a34b33e9276bc
	ips.exe	6c1bcf0b1297689c8c4c12cc70996a75
	isatapx64.zip	453810a77057d30f0ee7014978cdc404
	local.exe	08644155f5c8f94f0cc23942c5c5068f
	lstr.exe	623e4626d269324da62c0552289ae61f
	lstsrall.exe	290c26433a0d9d14f1252e46b1204643
	mmon.exe	db0450080be21ded08df8c897eb3bd9e
	mtmp.exe	e2db09553f23a8abc85633f6bf1a0b49
	netc.exe	322e136cb50db03e0d63eb2071da1ba7
	netc.exe	322e136cb50db03e0d63eb2071da1ba7
	notcp.exe	a35e944762f82aae556da453dcba20d1
	osql.exe	4b9b36800db395d8a95f331c4608e947
	osql.rll	df5dbcbcac6e6d12329f1bc8a5c4c0e9
	pmap.exe	814b88ca4ef695fea3faf11912a1c807
	portfwd.exe	d975fc6cda111c9eb560254d5eedbe0a
	psexec.exe	aeee996fd3484f28e5cd85fe26b6bdcd
	quark.zip	2cd8dddaf1a821eeff45649053672281
	svchosts.exe	2cd8dddaf1a821eeff45649053672281
	xmlrpc.php	c583bdcec14c6651cfd8a2a95736799d
	query.exe	a109c617ecc92c27e9dab972c8964cb4
	release.exe	f45f8df2f476910ee8502851f84d1a6e
	svchosts.exe	1d2f0491678fbc6858fff2a5d61d3003
	wmiislog.exe	e2db09553f23a8abc85633f6bf1a0b49
	svchosts.exe	c0c9c5e1f5a9c7a3a5043ad9c0afa5fd
	bcp.exe	3f00dd56b1dc9d9910a554023e868dac
	osql.exe	02137a937f6fbc66dbc59ab73f7b1d3e
	psexec.exe	aeee996fd3484f28e5cd85fe26b6bdcd
	bladelogic.exe	433a2750429d805907aa4848ff666163
	System32.exe	b9cf8e70681755c1711c38944695eeaa
	Svcsec.exe	25f7b169b43c4d5db472afb0ee09b035
	oposvc.exe	dd90c44afa5da730b8cb979667ae8fd3
	svchosts.exe	0561344c4e4460077fdc79a4679508ed

	Filename	MD5 Hash Value
Malware Signatures	rtcli.dll	4bd819d9e75e4e8ecf1a9599f44af12a
	mstdc.exe	57703973ff74503376a650224aa43dfa
	mstdc.bak	67ed156e118b9aa65ed414a79633a3d4
	msaudit.dll	27bfffa7d034a94b79d3e6ffdda50084
	mn32.exe	89a8844c1214e7fc977f026be675a92a
	si.vbs	40efe7632b01116eefaba438c9bcee34
	sd32.exe	9c3a1d3829c7a46d42d5a19fe05197f3
	TcpAdaptorService.exe	cfee737692e65e0b2a358748a39e3bee 85f94d85cfeff32fa18d55491e355d2b
	Osql.exe, svchosts.exe	4b9b36800db395d8a95f331c4608e947
	oposwin.exe	3446cd1f4bee2890afc2e8b9e9eb76a2
	svcmon.exe	0fff972080248406103f2093b6892134
	nYmTxGSJhLLFfagQ.bat	eae4718ea5a860cc372b5728e96af656
	tbcsvc.exe	1aa662d329cc7c51d2e9176024fedee8
	mssec.exe	d7e5e85ccb6c71a39b99a9228313cc33
	msproc.exe	2e567707730ed2c76b162a97dcf28c05

	IP	Description
Malicious IPs / Domains	89.35.148.67	Embedded within system32.exe
	examene.uvvg.ro	Embedded within svcsec.exe
	rghost.net	Russian file sharing web site. Note that some activity to this site might be legitimate