connect

Your Independent HP Business Technology Community

The Connection

A Journal for the HP Business Technology Community

The Targeted Attack on Target: Lessons to Learn

Neutralize Data Breaches

Protect your Data and your Brand

Show Some Integrity... Check Your Files!

Mar – Apr 2014 | Volume 35, No. 2

Neutralize Data Breaches

Protect your Data and your Brand

Carole Murphy
Director, SecureData
Voltage Security, Inc.

Even the simplest payment process requires payment card data to be captured, transmitted, stored, and processed across many high risk systems, applications, and links in the ecosystem. As we have seen, attackers will take full advantage of any vulnerability or point in the chain where data is available in live form to steal and monetize. Recent events have shown a dramatic rise in sophisticated threats to IT infrastructure by cyber-thieves looking to steal sensitive data from systems that are always on and always connected.

On the news of multiple attacks beginning with the Target data breach during the 2013 Holiday Shopping season, Mark Bower, Vice President for Product Management and Solutions Architecture at Voltage Security, said, "The news of infiltration of IT systems leading to the loss of personal data strongly indicates that the breach is in more than the POS systems, and likely in upstream IT platforms. The personal data stolen in the second wave of reports has the signature of a typical customer loyalty or customer profile database."

Early in 2013, Visa began sending alerts to retailers about new malware variants capable of stealing data from memory in POS environments. While there are likely variations, the root cause appears to be the same–the ability to steal track data straight out of the authorization flow, even if traditional database encryption was used on the POS for PCI Compliance.

Typically there are two points in the retail chain where attacks take place – the POS or the payment switching back end. POS systems are often the weak link in the chain and vulnerable. They often run a standard OS and are thus subject to exploits and zero-day attacks if exposed to a malware delivery channel such as a browser, a compromised POS management system, patch system or worse, an insider. In use, POS systems should be isolated from other networks to restrict access to payment data flows, but often, they are connected to many systems. As a POS and checkout are in constant use especially around high volume periods like Black Friday, they are less frequently patched and updated and thus vulnerable to malware compromise impacting massive amounts of cardholder data.

How the malware arrived in Target's POS systems has been traced back to an initial intrusion with network credentials stolen from a third-party vendor. But the vector can be anything from hops from corporate systems, to email attachments leading to credential stealing, to insiders, and other tactics prior to a full compromise.

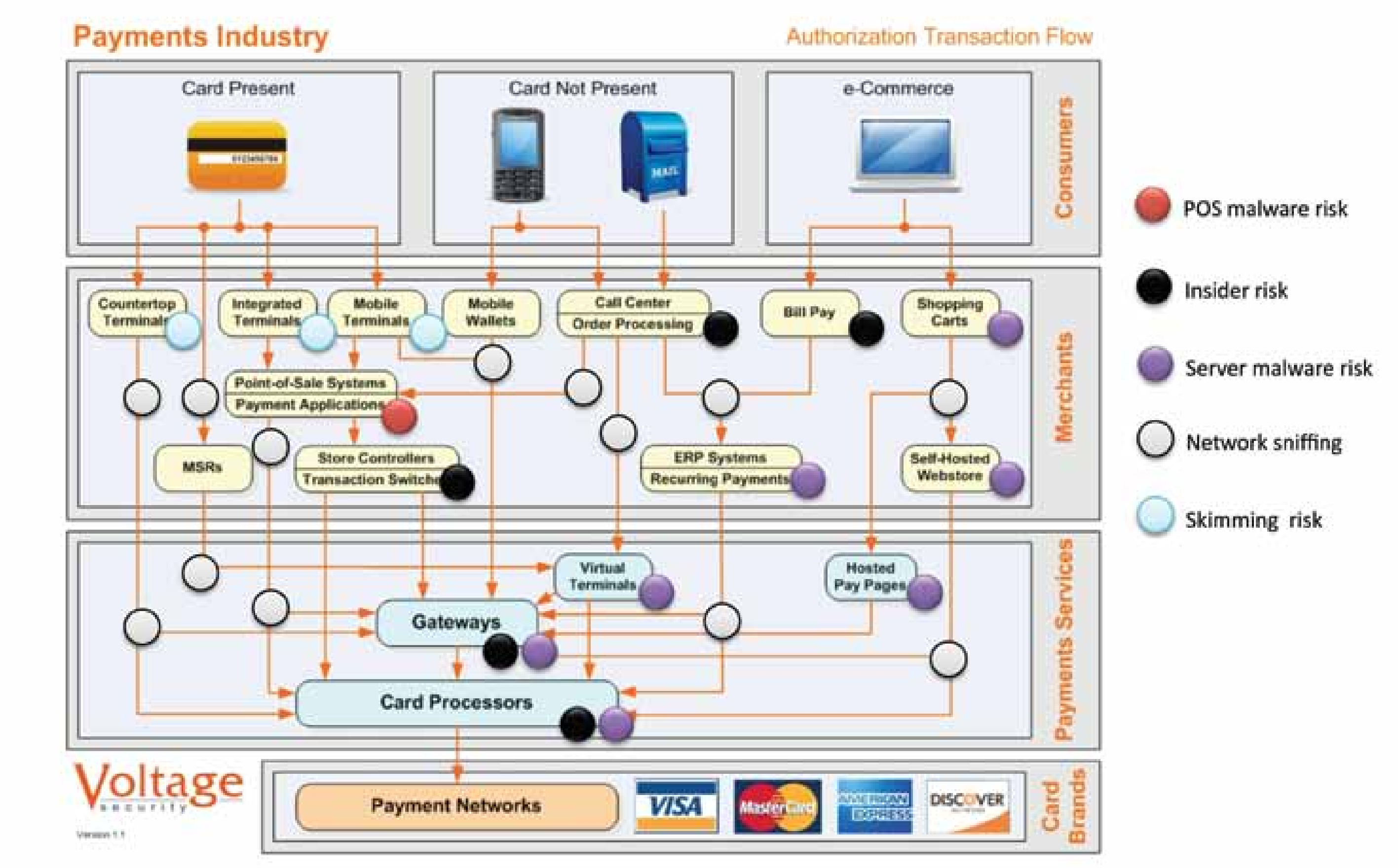
Terence Spies, CTO at Voltage, recently commented that, "Attacks that move in multiple phases are not unusual at all. Attackers typically move in a pattern of using public or easily accessible data to understand the targeted network and the machines operating on that network, then start probing machines on the outside of the network as a point of access for malware, then leverage the access on those machines into more sensitive assets. The RSA breach is another example of this kind of attack, where email malware infected employee laptops, then waited to propagate to more sensitive machines. In this case, using an internal file share to store information harvested off the POS machines would be a pretty typical kind of strategy, as it allows the attacker to control how and when the data is exfiltrated, and eliminates the need for a continual connection to the compromised POS terminals."

Even with the best intentions, traditional monitoring and data protection strategies, including conventional data-at-rest encryption, aren't providing the answers that retailers, financial service providers, and e-commerce businesses need. The challenge in the enterprise and in the payments ecosystem is to protect data wherever it goes, over its whole lifecycle. To neutralize a data breach, the goal is never to yield live data that can be monetized. If protected data is compromised, the attacker gets nothing of value. The good news is that there is a way to achieve this level of protection, very efficiently, by implementing data-centric security.

When people think about encryption, they often think about protecting the disk, the database, or the network, using point approaches. But these approaches don't protect data over its life, or in transit. As data moves from storage to databases into applications, there are gaps where it can be exploited, including data left in the clear, in memory. With data-centric security, you put security with the data itself, like the credit card number, the track data, or even the EMV or personal data in loyalty systems. With data-centric encryption, the field is protected (using techniques like Format-Preserving Encryption) the instant the data is captured–for example, before it hits the POS. By preserving format, the POS can still use the data in its protected form without decryption. See NIST draft standard 800-38G (**http://csrc.nist.gov/publications/drafts/800-38g/sp800_38g_draft.pdf**) for additional information on Format-Preserving Encryption.

Tokenization, which is used as a way of replacing credit card numbers with randomly generated replacement values, is one of the data protection and audit scope reduction methods recommended by the PCI DSS. By tokenizing payment card data the scope of the PCI audit and cardholder data environment is limited because the storage of payment cards is being substituted by tokens. The footprint for attacks shrinks accordingly because token data is useless if stolen. Tokenization has emerged as a powerful technique for removing live data from systems while achieving PCI scope reduction. Tokenization replaces live values with a random value that only the tokenization system or service can map to authorized applications or services.

Card Data Risks in the Merchant Ecosystem



What's needed to protect against adaptive, persistent cyber-threats, is a data-centric approach to protect data going up to the trusted host, and also, to remove live data in back-end systems. Point-to-point encryption (P2PE) from the instant the card data is read, also called end-to-end encryption, encrypts all the payment card data before it even gets to the POS, and has become part of the PCI recommendations, echoed by Visa. If the POS is breached, the data will be useless to the attacker. Tokenization can eliminate live data from post-authorization retail processes like warranty and returns yet enable the retail business to still operate as before – even at Black Friday scale. Data-centric encryption and tokenization together form a very strong defense.

Voltage Security offers data-centric solutions, including Voltage Format-Preserving Encryption™ (FPE™), and recently announced the General Availability of Voltage Secure Stateless Tokenization™ (SST™) for native tokenization on the HP NonStop OS. Voltage SST on HP NonStop allows fully native tokenization without requiring separate Web Service calls, permitting full speed operation. A single operation can now be used to both decrypt and tokenize incoming Primary Account Number (PAN) data. This single operation reduces latency by eliminating the need to send tokenization requests to a separate server.

With EMV on the horizon to make it much harder to counterfeit physical cards from stolen data, and with P2PE and Tokenization to protect the card data in the retail flow, merchants and enterprises can turn the tables on data breaches in a major way. With the significant reduction in the cost of PCI compliance, there's a strong ROI to justify it–in addition to avoiding the cost and complications of fines, remediation, and brand damage, as in this case.

Carole Murphy is responsible for developing market strategy for Voltage Security's SecureData product line and related solutions, including go-to-market planning, product communication, positioning and market awareness. She has over 25 years of experience spanning the security, networking, and IT service management industries.