Under the Hood of the IBM Threat Protection System

The Nuts and Bolts of the Dynamic Attack Chain

You are an...

IT Security Manager at a global retailer with 600 locations.

You manage a team of IT analysts that are responsible for maintaining network operations for point of sale in retail locations, central servers, the company website and mobile applications.

Other areas of your company, like product management, have credentials for various applications to enable them to conduct business.

Monday 8:30am

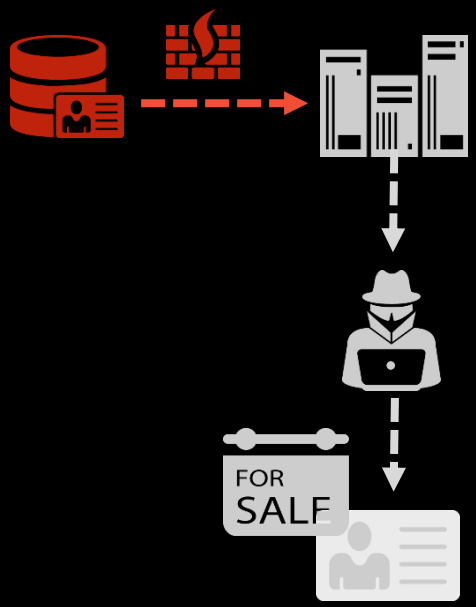
Over a cup of coffee, you get a phone call from a well-known security blogger that your customer credit card numbers and one of your Internet-accessible server addresses showed up on an underground forum known for trading stolen information.

Within 10 minutes, you notify legal counsel, the CIO, and law enforcement and begin a forensics investigation to figure out how the breach occurred.

The previous Saturday

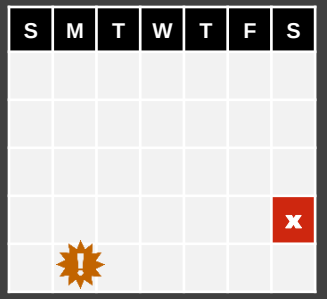
Investigating the server logs from the weekend shows a connection from a POS server to an external FTP server you don't recognize, hosted at the dynamic domain 1337.my-ftp.biz.

The attacker must have manually copied excerpts of the data from the FTP server to the underground forum.



IBM Threat Protection System:

- Prevent
- Detect
- Respond

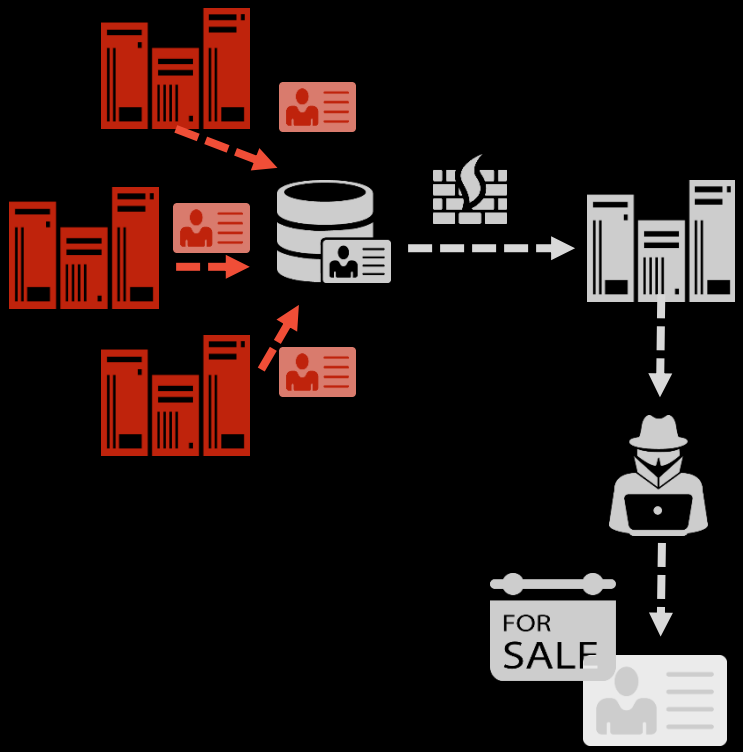


Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- Gather
- **Exfiltrate**

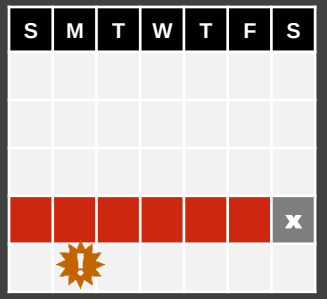
The previous week

You find evidence in the log files of transfers of PII in the previous week from POS servers to a single internal server, the server that connected to the external FTP server.



IBM Threat Protection System:

- Prevent
- Detect
- Respond

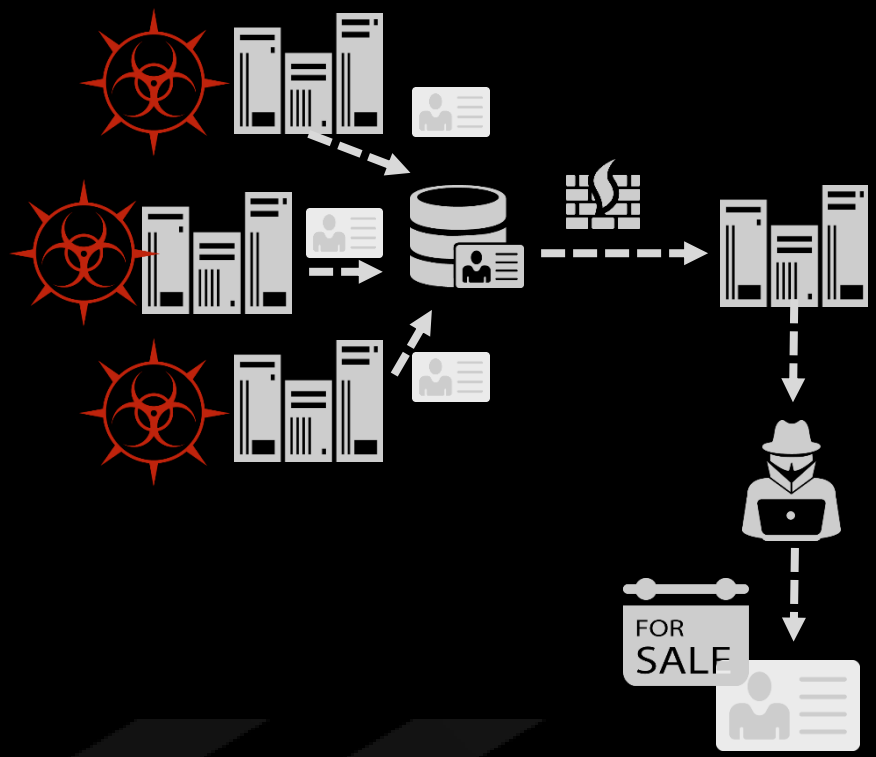


Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- **Gather**
- Exfiltrate

The previous 2-3 weeks

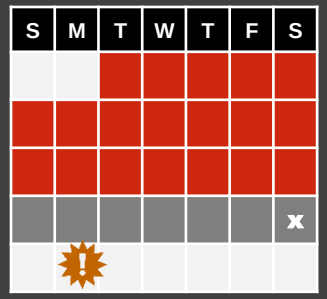
You find a copy of the file CardScraper.exe on each of the POS servers that sent PII to the server that made the external connection.



In the 2-3 week prior, that malware hunted for additional POS servers, copying toolchains and password crackers to them, and infiltrating the network.

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- Latch-on
- **Expand**
- Gather
- Exfiltrate

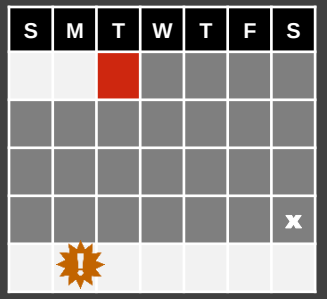
28 days earlier

Probing further, you find a RAT (Remote Access Trojan) named svch0st.exe, which acted as a dropper to secretly install, execute, and avoid anti-virus detection.

This program downloaded CardScraper.exe from an external server located at IP Address 91.216.73.32 and copied it to the POS servers.

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- **Latch-on**
- Expand
- Gather
- Exfiltrate

29 days earlier

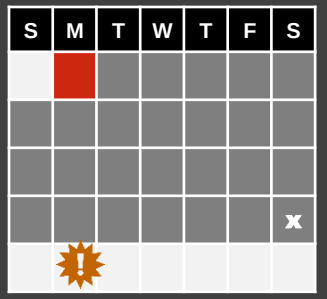
While working in a coffee shop, Dan, in Development, receives an email from a retailer requesting account verification.

He clicked the link, but didn't notice it was to fake website named acccount-verify.com, which launched a zero-day exploit to his browser and downloaded the trojan svch0st.exe to his system.

Dan drives to work where he logs into the network, allowing svch0st.exe to slip into the network and start the chain of events leading to the breach.

IBM Threat Protection System:

- Prevent
- Detect
- Respond



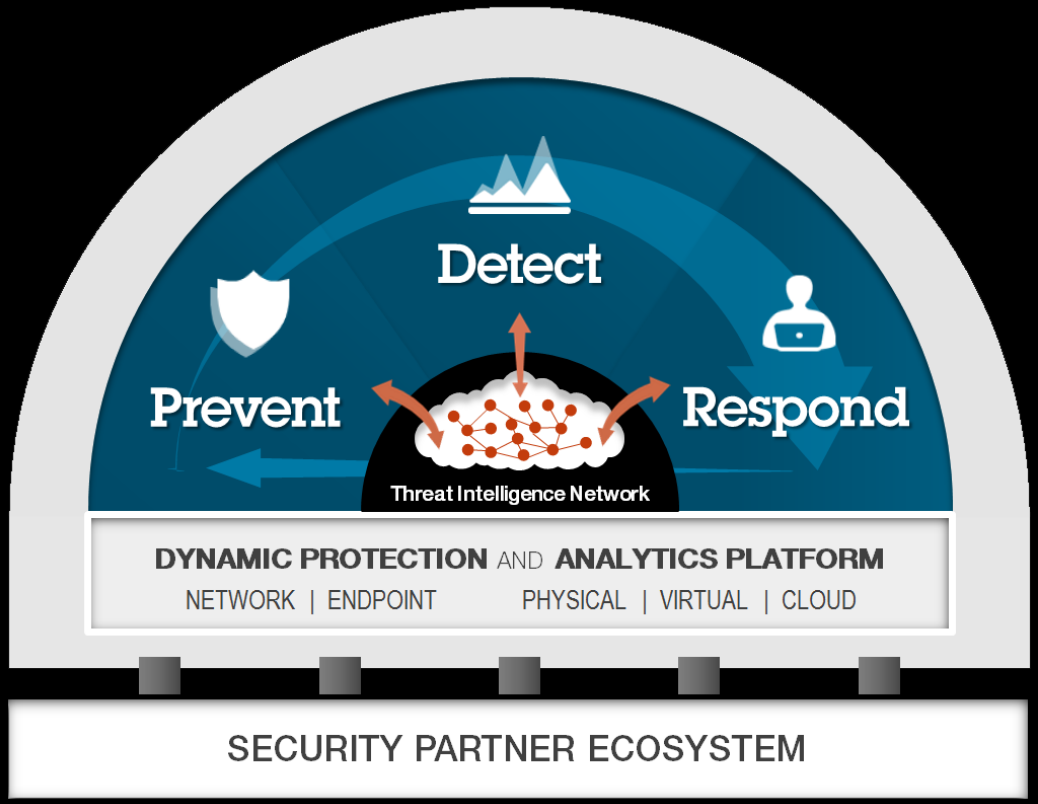
Attack Chain Stage:

- **Break-In**
- Latch-on
- Expand
- Gather
- Exfiltrate

Let's start from the beginning to see how the attack could have been disrupted...

IBM Threat Protection System

A dynamic, integrated system to disrupt the entire lifecycle of advanced attacks



Smarter Prevention

Stop unknown threats with behavioral-based defenses on both the endpoint and network

Security Intelligence

Automatically detect weaknesses and anomalies with enterprise-wide visibility and insights

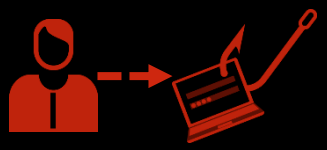
Continuous Response

Quickly understand incidents and use findings to strengthen real-time defenses

Open Integrations

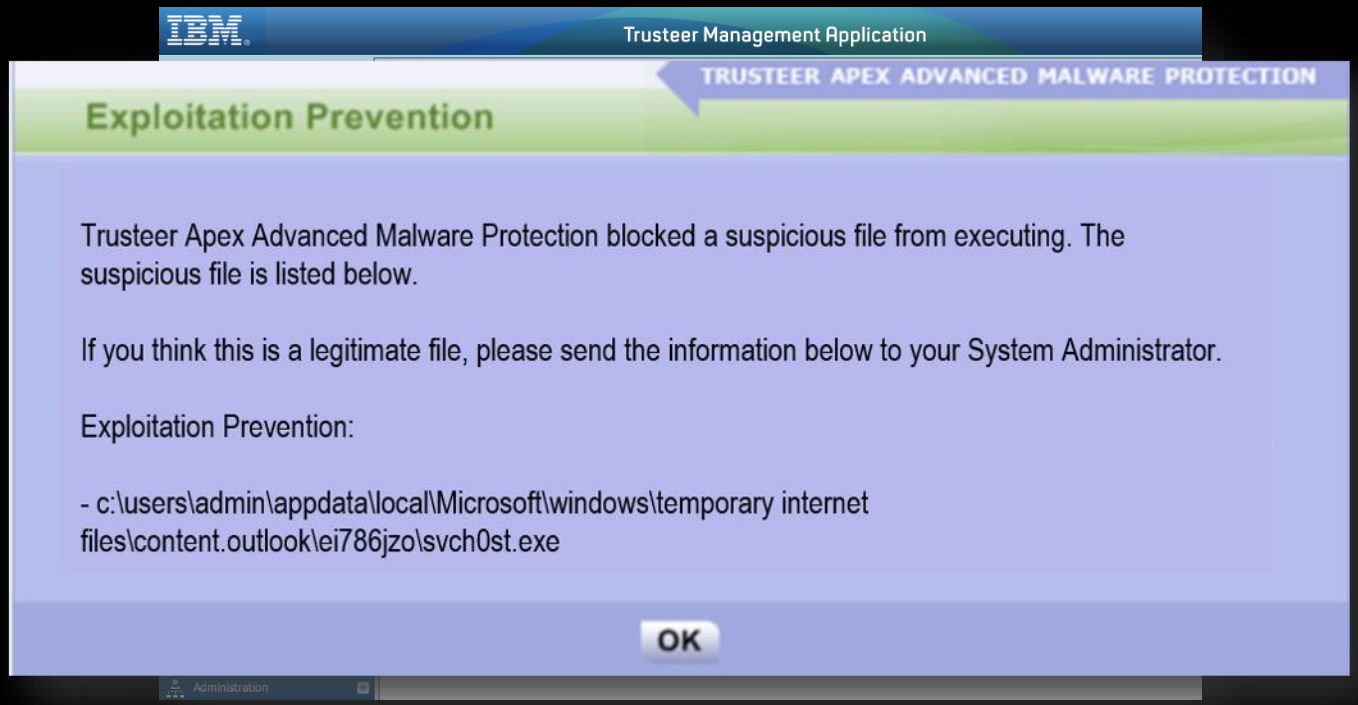
Share context between domains and third party products using an open platform and ecosystem

29 days earlier



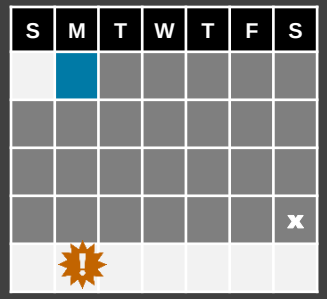
Dan is the subject of a phishing scam and inadvertently downloads malware

IBM Security Trusteer Apex Advanced Malware Protection stops the zero-day exploit from attacking his web browser and executing the RAT named “svch0st.exe”



IBM Threat Protection System:

- **Prevent**
- Detect
- Respond



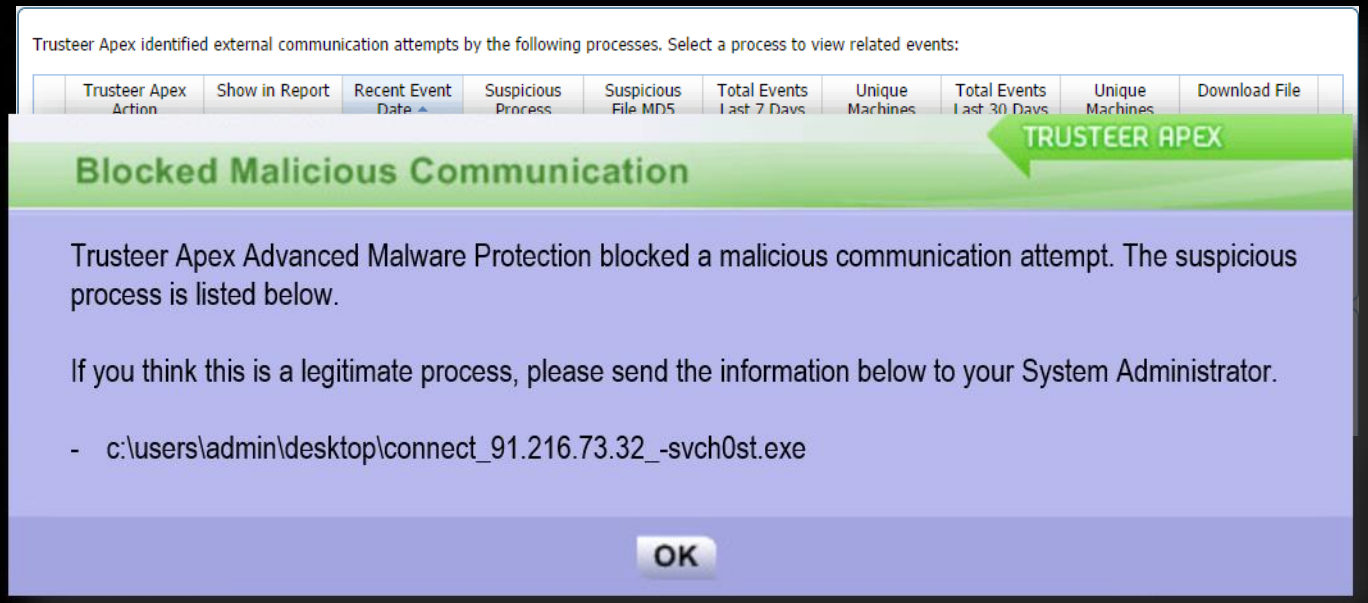
Attack Chain Stage:

- **Break-In**
- Latch-on
- Expand
- Gather
- Exfiltrate

28 days earlier

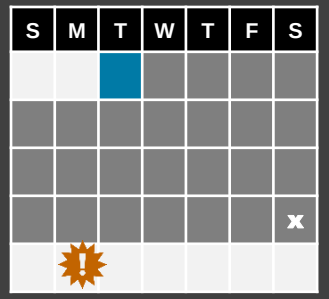
The RAT downloads CardScraper.exe and the malware starts to replicate

Trusteer Apex blocks command & control (C&C) activity on the endpoint, stopping the RAT from communicating with the server to download CardScraper.exe



IBM Threat Protection System:

- **Prevent**
- Detect
- Respond



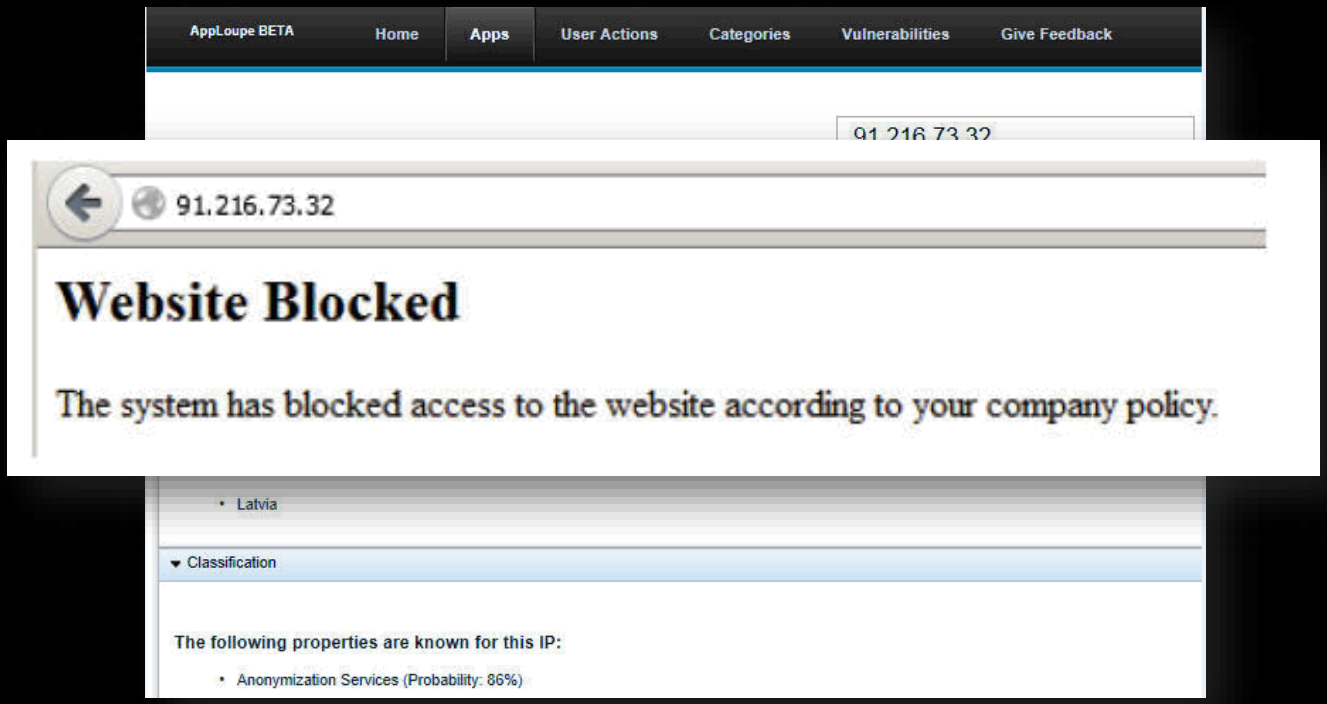
Attack Chain Stage:

- **Break-In**
- **Latch-on**
- **Expand**
- **Gather**
- **Exfiltrate**

28 days earlier

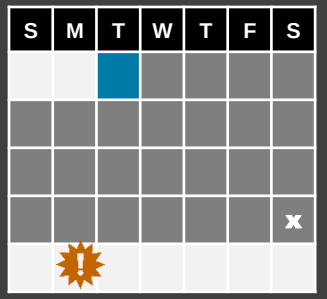
The RAT downloads CardScraper.exe and the malware starts to replicate

IBM Security Network Protection prevents C&C activity on the server by blocking the remote IP 91.216.73.32 hosting CardScraper.exe based on IP reputation



IBM Threat Protection System:

- **Prevent**
- **Detect**
- **Respond**



Attack Chain Stage:

- **Break-In**
- **Latch-on**
- **Expand**
- **Gather**
- **Exfiltrate**

28 days earlier

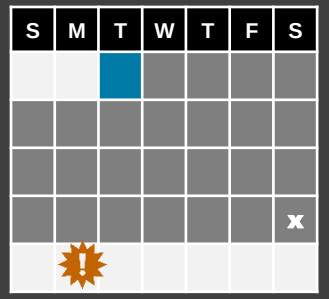
The RAT downloads CardScraper.exe and the malware starts to replicate

IBM QRadar SIEM detects the RAT install from system event logs, giving it a magnitude score of 8 and raising a flag in the security analyst's dashboard

Event Information			
Event Name	HTTP:HOTMAIL:EXE-DOWNLOAD		
Low Level Category	Executable Code Detected		
Event Description	HTTP: MSN Hotmail Executable File Extension Download		
Magnitude	(8)	Relevance	10
Username	N/A		
Start Time	Oct 20, 2013, 7:22:48 PM	Storage Time	Oct 20, 2013, 7:22:48 PM
Executable (custom)	CardScraper.exe		

IBM Threat Protection System:

- Prevent
- **Detect**
- Respond



Attack Chain Stage:

- Break-In
- **Latch-on**
- Expand
- Gather
- Exfiltrate

2-3 weeks earlier

CardScraper.exe is copied to POS servers throughout the business

IBM QRadar SIEM detects file transfers based on network events, and reports a policy violation on unauthorized access to a POS server

Id	Description	Offense Type	Offense Source	Magnitude
1471	Multiple Login Failures for the Same User containing Root Login Failed	Username	root	
2661	Policy Violation: Unauthorized Access to POS Server	Source IP	10.0.110.123	
1458	Assess potential inbound connections from the internet to regulatory assets	Event Name	Assess potential inboun...	
1463	Assess actual inbound connections from the Internet to regulatory assets	Event Name	Assess actual inbound c...	
1482	Potentially Successful Exploit preceded by Exploit Followed by Suspicious Ho...	Source IP	10.0.240.4	
1511	Attack Followed by an Attack Response preceded by Policy: Chat or IM Traffic...	Source IP	10.0.230.231	

Destination Network is Server_Network POS_Servers (Clear Filter)

Current Statistics

Top 10 Destination IP:Source IP Results By Total Bytes (Sum)

10/20/13 6:12 PM - 10/20/13 6:42 PM

25 % 25 % 25 % 25 %

Legend

10.0.120.40:10.0.240.39 10.0.120.20:10.0.110.120 10.0.120.10:10.0.110.42 10.0.120.10:10.0.240.151

Top 10 Destination IP:Source IP Results By Total Bytes (Sum)

10/20/13 6:12 PM - 10/20/13 6:42 PM

60M 40M 20M 0

Legend

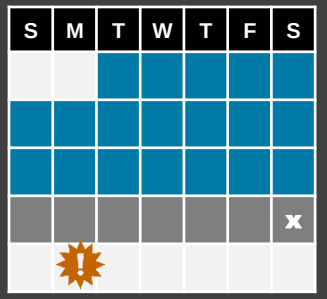
10.0.120.40:10.0.240.39 10.0.120.20:10.0.110.120 10.0.120.10:10.0.110.42 10.0.120.10:10.0.240.151

(Hide Charts)

Destination IP	Source IP	Source Network (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Application (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)
10.0.120.40	10.0.240.39	Users_1	445	POS_Servers	DataTransfer.WindowsFileSharing	1,194,478	38,464,756	39,659,234	13,033	28,329	41,362
10.0.120.20	10.0.110.120	Users-2	445	POS_Servers	DataTransfer.WindowsFileSharing	1,194,478	38,464,756	39,659,234	13,033	28,329	41,362
10.0.120.10	10.0.110.42	Users-2	445	POS_Servers	DataTransfer.WindowsFileSharing	1,194,478	38,464,756	39,659,234	13,033	28,329	41,362
10.0.120.10	10.0.240.151	Users_1	445	POS_Servers	DataTransfer.WindowsFileSharing	1,190,044	38,460,832	39,650,876	13,011	28,308	41,319

IBM Threat Protection System:

- Prevent
- **Detect**
- Respond



Attack Chain Stage:

- Break-In
- Latch-on
- **Expand**
- Gather
- Exfiltrate

The previous week

PII was transferred from infected POS servers to a single server

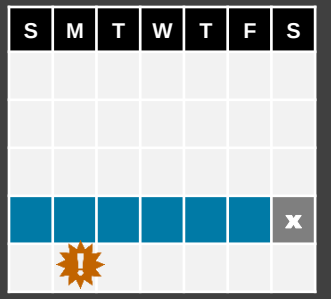
IBM Security Network Protection (XGS) detects and blocks the transfer of the credit card number files

Tag Name	Status	Severity	Event Count	Source Count	Target Count
Content_Analyzer_Credit_Card_Num	Detected event	Low	1	1	1
System	Detected event	Low	19	2	2
HTTP_Get	Detected event	Low	6	1	1
EventCollector_Info	Detected event	Low	39	1	1

Tag Name	Status
Content_Analyzer_Credit_Card_Num	Detected event

IBM Threat Protection System:

- (●) Prevent
- ( ) Detect
- ( ) Respond



Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- **Gather**
- Exfiltrate

The previous week

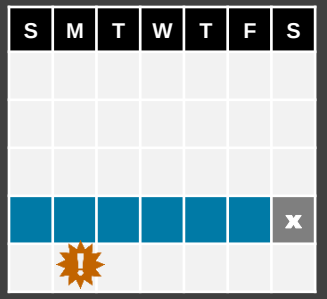
PII was transferred from infected POS servers to a single server

IBM QRadar SIEM detects communication behavior that deviates from corporate and compliance policies

Source IP	Source Network	Source Port	Destination IP	Destination Port	Protocol	Application
10.0.110.37	POS_Server	64935	151.56.78.9	20	udp_ip	DataTransfer.FTP
10.0.110.120	POS_Server	64935	151.56.78.9	20	udp_ip	DataTransfer.FTP

IBM Threat Protection System:

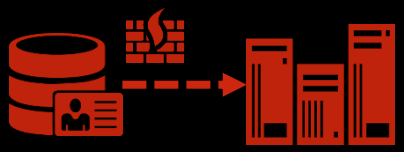
- Prevent
- **Detect**
- Respond



Attack Chain Stage:

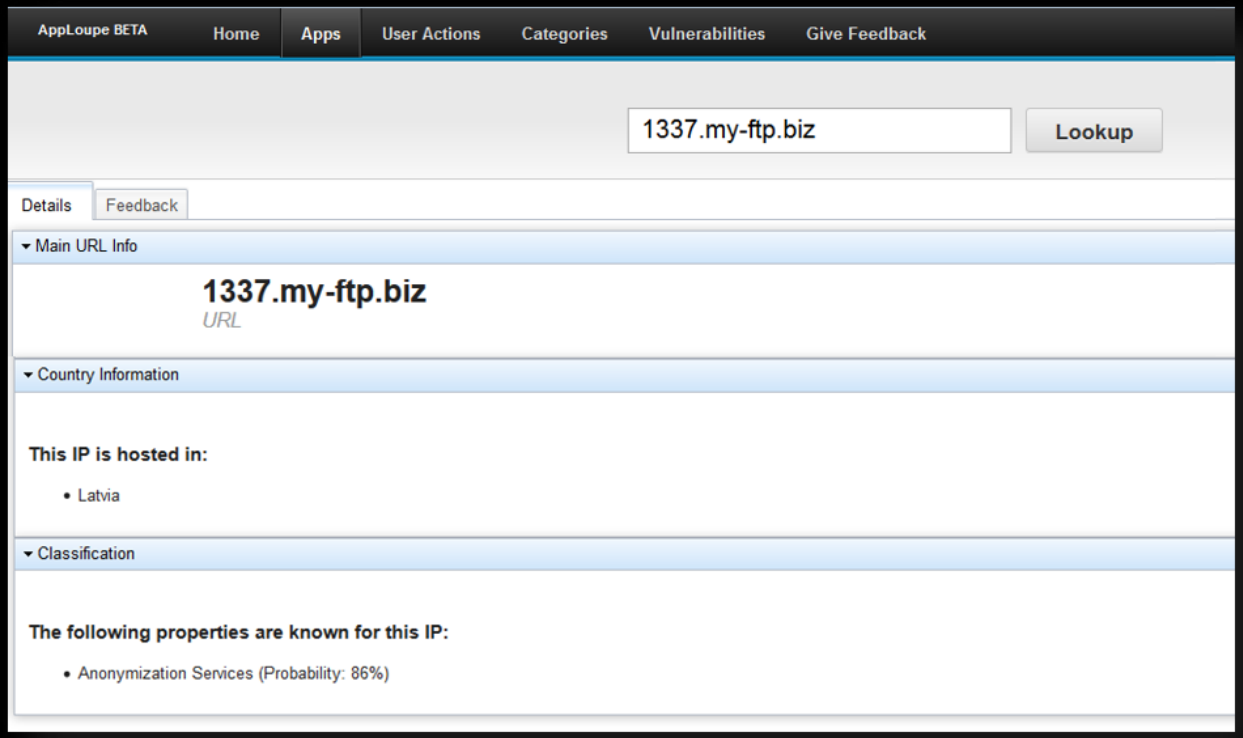
- Break-In
- Latch-on
- Expand
- **Gather**
- Exfiltrate

The previous Saturday



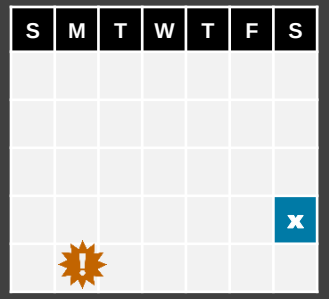
A POS server connects to an unknown external FTP server and the PII is exfiltrated.

IBM Security Network Protection XGS would block the outbound connection based on the URL reputation of remote FTP server “1337.my-ftp.biz”



IBM Threat Protection System:

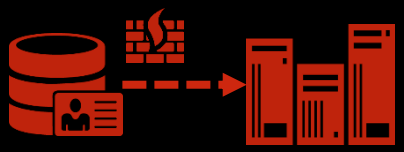
- **Prevent**
- **Detect**
- **Respond**



Attack Chain Stage:

- **Break-In**
- **Latch-on**
- **Expand**
- **Gather**
- **Exfiltrate**

The previous Saturday



A POS server connects to an unknown external FTP server and the PII is exfiltrated.

IBM QRadar SIEM would detect anomalous flow out from a server that never connected outbound before with a "Connection Outbound to Internet from Critical Asset" flag

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs
1471	Multiple Login Failures for the Same User containing Root Login Failed	Username	root		Multiple (10)
1458	Assess potential inbound connections from the internet to regulatory assets	Event Name	Assess potential inboun...		Multiple (5)
1463	Assess actual inbound connections from the Internet to regulatory assets	Event Name	Assess actual inbound c...		Multiple (5)
2670	Anomaly Detection: Connection Outbound to Internet from Critical Asset	Source IP	10.0.120.50		10.0.120.50
1482	Potentially Successful Exploit preceded by Exploit Followed by Suspicious Host Activity - Chained preceded by Multiple Vect...	Source IP	10.0.240.4		dhcp-4-users-1.ac...
1511	Attack Followed by an Attack Response preceded by Policy: Chat or IM Traffic Detected preceded by Exploit Followed by Su...	Source IP	10.0.230.231		dhcp-231-vpn.acm...
1461	Compliance: assess regulatory assets using insecure protocols	Event Name	Compliance: assess reg...		Multiple (5)

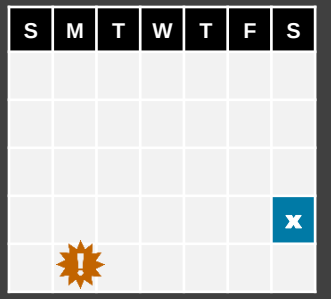
Assess actual inbound connections from the Internet to regulatory assets

Anomaly Detection: Connection Outbound to Internet from Critical Asset

Potentially Successful Exploit preceded by Exploit Followed by Suspicious Host Activity - Chained preceded by Multiple Vect... Source IP 10.0.240.4 dhcp-4-users-1.ac...

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- Gather
- **Exfiltrate**

How do you conduct this forensics investigation?

With a solution like QRadar Incident Forensics, you can…

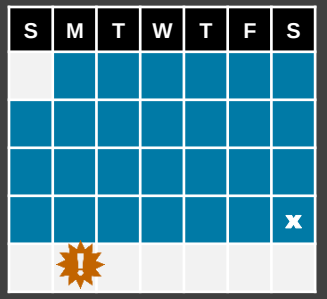
- Query external server addresses found on the underground forum
- Report internal connections
- Show external file transfers
- Identify malware transferred by the attacker
- Discover connection histories and extended relationships with internal assets and identities

IBM Security
QRadar Incident Forensics

…via deep analysis and reconstruction of recorded packet capture files. Directly from the QRadar console.

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- Gather
- Exfiltrate

Early detection and rapid response are also critical

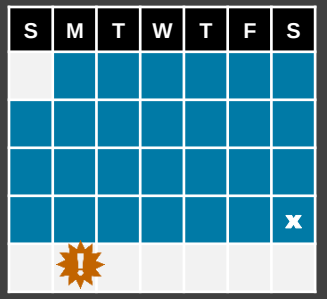
It can take just minutes to compromise your network, but months to discover and recover.

IBM offers Emergency Response Services to help.

- A team of incident response and forensics experts ready to respond globally
- 120 staff hours per year, which can be utilized for emergency response services or preventative services
- Unlimited emergency declarations
- Access to the X-Force Threat Analysis Service backed by global intelligence research
- Quarterly checkpoint, support, and update on threat landscape

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- Gather
- Exfiltrate

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY

Thank You

www.ibm.com/security