Under the Hood of the IBM Threat Protection System

The Nuts and Bolts of the Dynamic Attack Chain

Diana Kelley

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

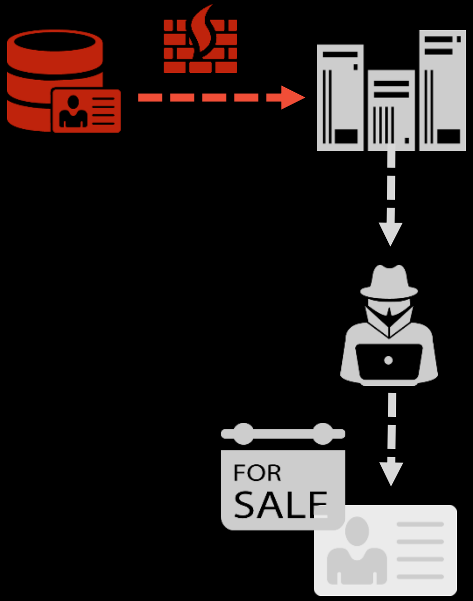
Over a cup of coffee, you get a phone call from a well-known security blogger that your customer credit card numbers and one of your Internet-accessible server addresses showed up on an underground forum known for trading stolen information.

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

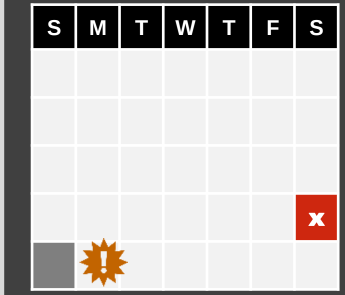
Investigating the server logs from the weekend shows a connection from a server to an external FTP server you don’t recognize, hosted at the dynamic domain 1337.my-ftp.biz.

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

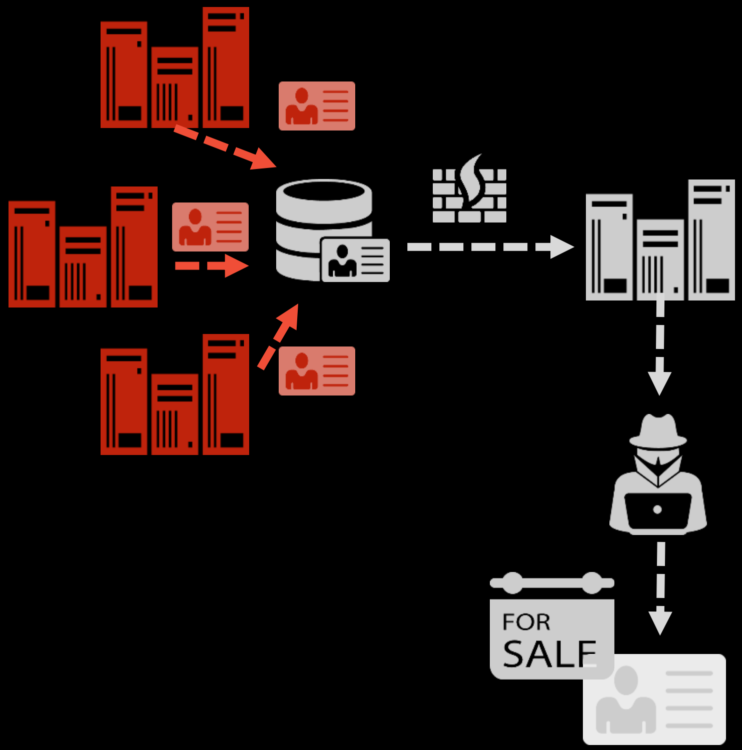
Expand

Gather

Exfiltrate

The previous week

You find evidence in the log files of transfers of PCI 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

S	M	T	W	T	F	S
🟥	🟥	🟥	🟥	🟥	🟥	x
▨	!					

Attack Chain Stage:

Break-In

Latch-on

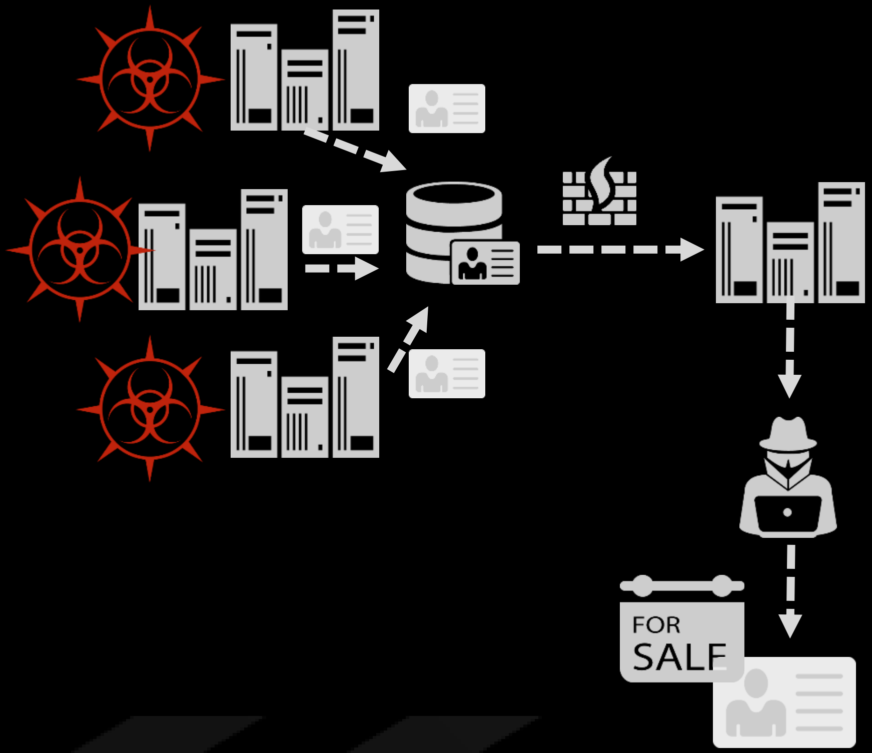
Expand

Gather

Exfiltrate

The previous 2-3 weeks

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



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

IBM Threat Protection System:

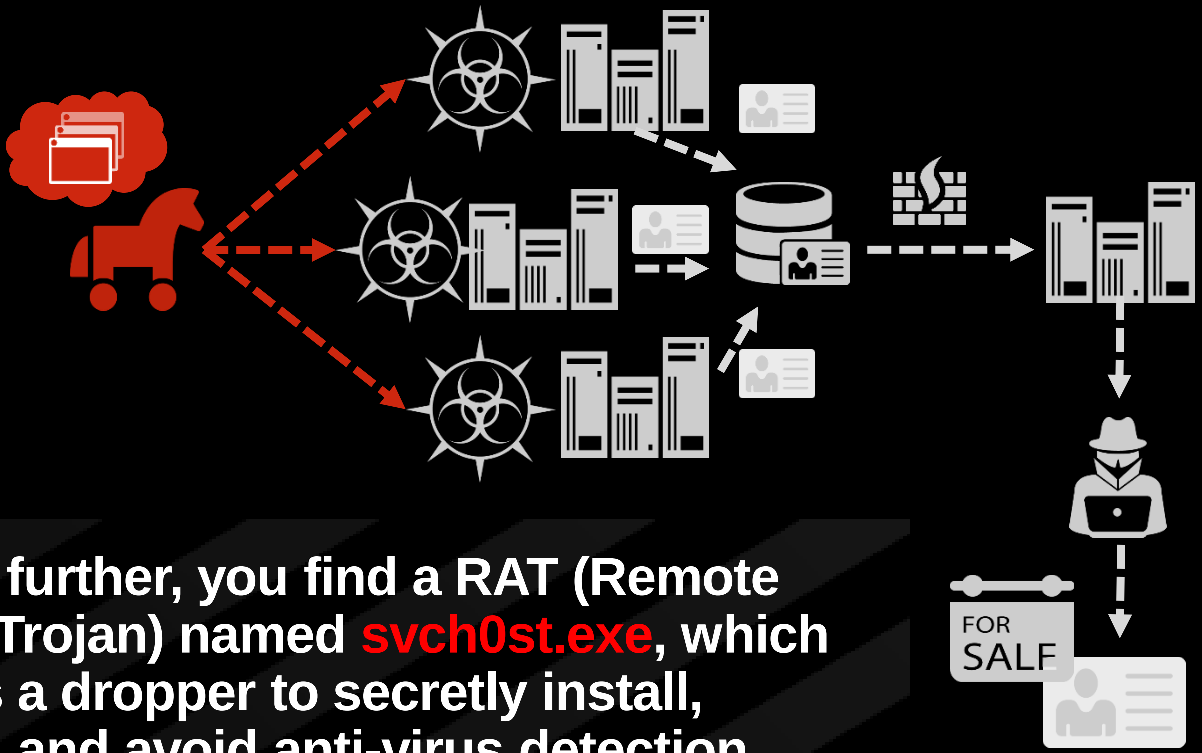
- ● Prevent
- ● Detect
- ● Respond

S	M	T	W	T	F	S
⬜	⬜	🟥	🟥	🟥	🟥	🟥
🟥	🟥	🟥	🟥	🟥	🟥	🟥
🟥	🟥	🟥	🟥	🟥	🟥	🟥
▨	▨	▨	▨	▨	▨	x
▨	!	⬜	⬜	⬜	⬜	⬜

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:

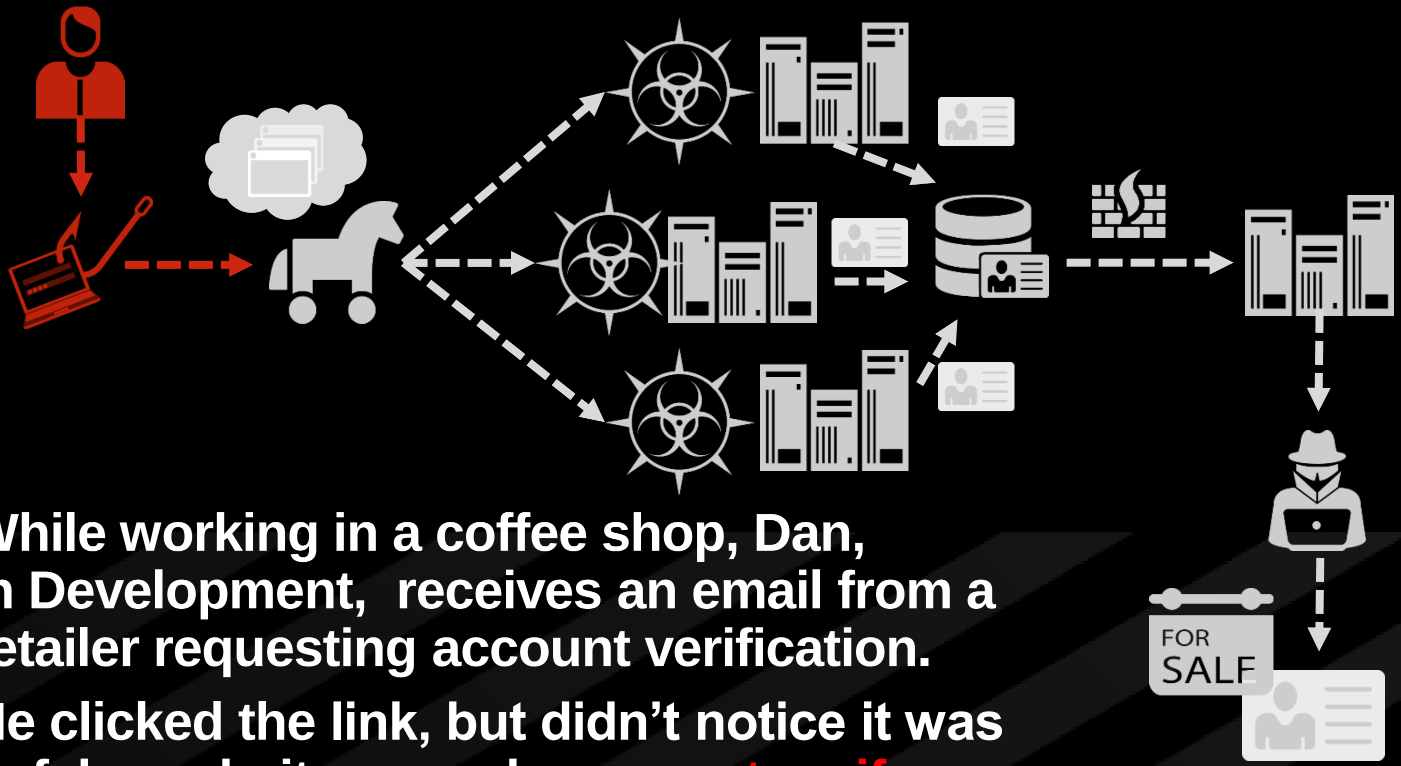
- ● Prevent
- ● Detect
- ● Respond

S	M	T	W	T	F	S
		🟥				
						x
	!					

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

S	M	T	W	T	F	S
	🟥					
						x
	!					

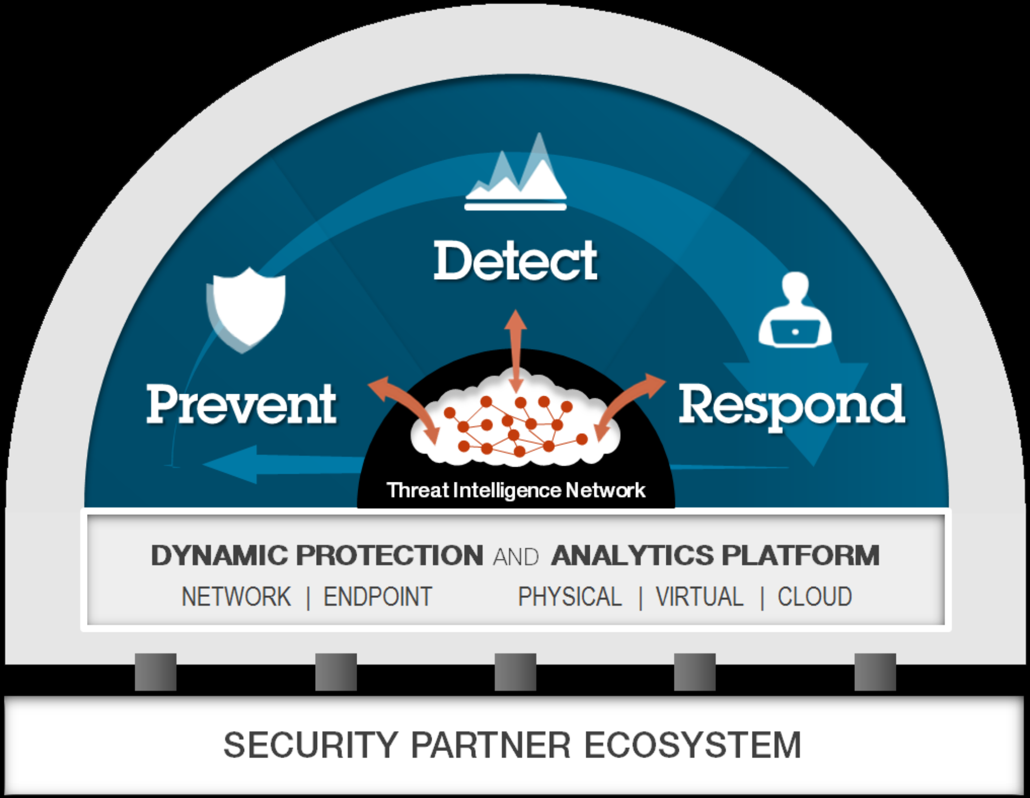
Attack Chain Stage:

- 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


Detect
Prevent
Respond
Threat Intelligence Network
DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD
SECURITY PARTNER ECOSYSTEM

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

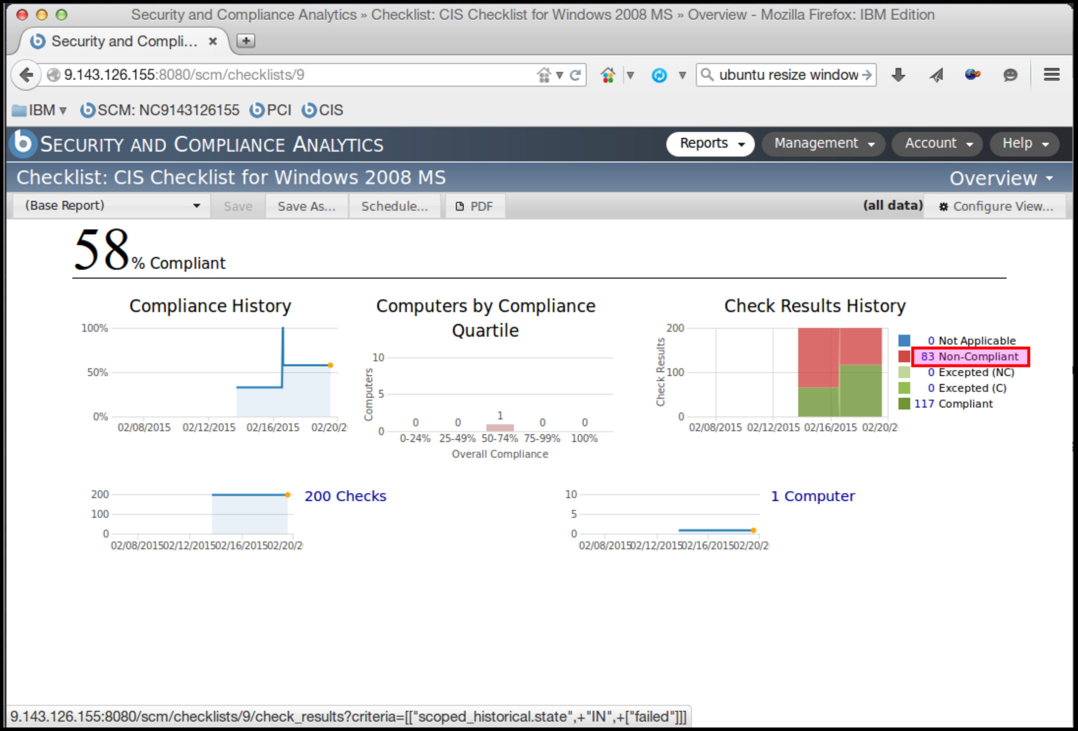
Continuous Response
Quickly understand incidents and use findings to strengthen real-time defenses

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

30+ days earlier

Prevention measures are in place to identify and remediate exposure for the company.

IBM Endpoint Manager identifies and manages policy exceptions on endpoints to quarantine and mark assets for remediation before the attack occurs.



Security and Compliance Analytics » Checklist: CIS Checklist for Windows 2008 MS » Overview - Mozilla Firefox: IBM Edition

Security and Compli...

9.143.126.155:8080/scm/checklists/9

ubuntu resize window

IBM ▾ SCM: NC9143126155 PCI CIS

SECURITY AND COMPLIANCE ANALYTICS

Checklist: CIS Checklist for Windows 2008 MS

Overview

(Base Report)

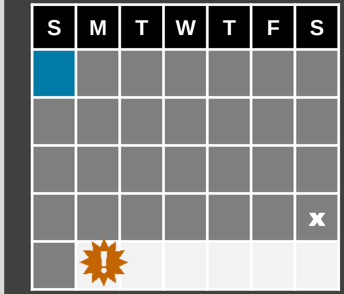
(all data)

58% Compliant

9.143.126.155:8080/scm/checklists/9/check_results?criteria=[["scoped_historical.state",+"IN",+["failed"]]]

IBM Threat Protection System:

- ● **Prevent**
- ○ **Detect**
- ○ **Respond**



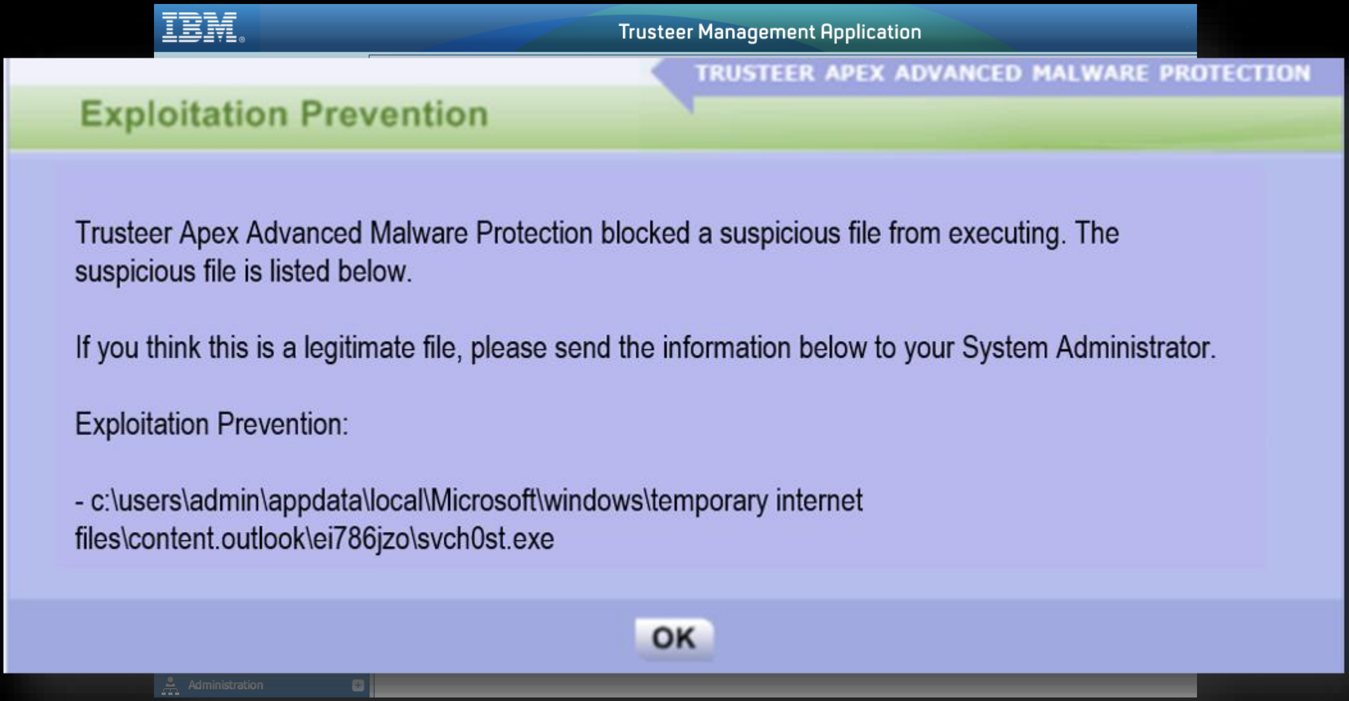
Attack Chain Stage:

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

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
Trusteer Management Application
TRUSTEER APEX ADVANCED MALWARE PROTECTION
Administration

Exploitation Prevention

Trusteer Apex Advanced Malware Protection blocked a suspicious file from executing. The suspicious file is listed below.

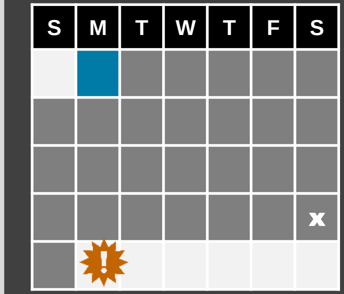
If you think this is a legitimate file, please send the information below to your System Administrator.

Exploitation Prevention:

- c:\users\admin\appdata\local\Microsoft\windows\temporary internet files\content.outlook\ei786jzo\svch0st.exe

IBM Threat Protection System:

● Prevent
○ Detect
○ Respond



Attack Chain Stage:

Break-In

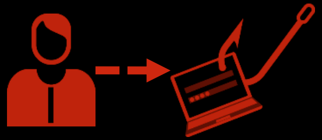
Latch-on

Expand

Gather

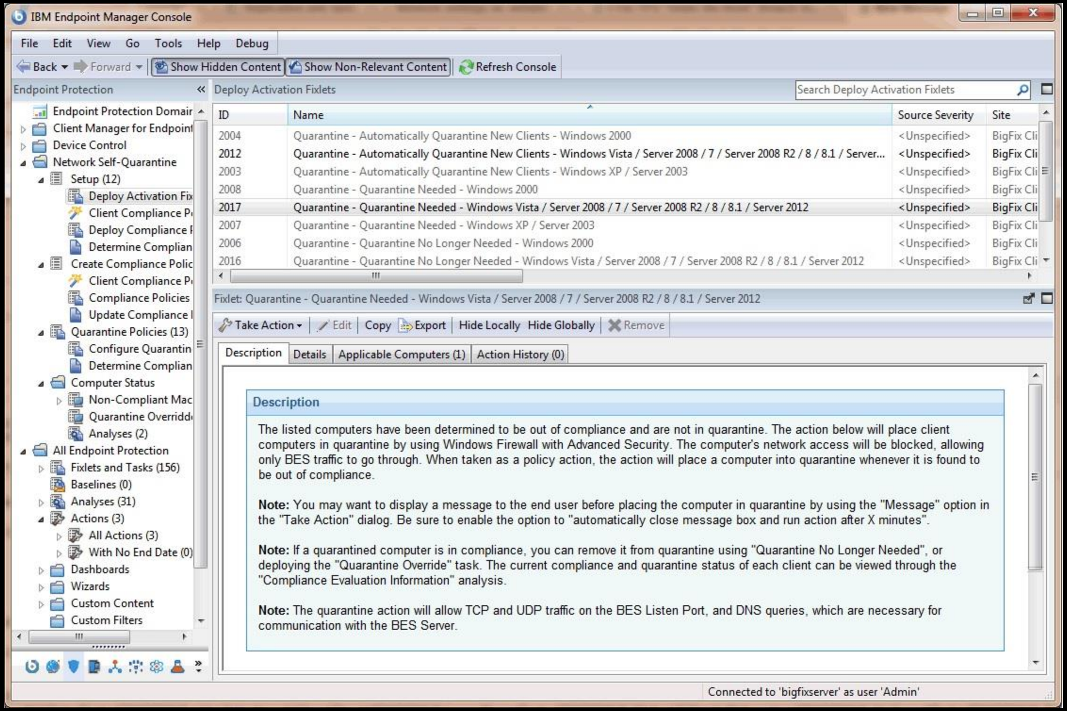
Exfiltrate

29 days earlier



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

Based on the output from Trusteer Apex, IBM Endpoint Manager quarantines Dan’s laptop so that it can only communicate with IEM to be remediated



ID	Name	Source Severity	Site
2004	Quarantine - Automatically Quarantine New Clients - Windows 2000	<Unspecified>	BigFix Cli
2012	Quarantine - Automatically Quarantine New Clients - Windows Vista / Server 2008 / 7 / Server 2008 R2 / 8 / 8.1 / Server...	<Unspecified>	BigFix Cli
2003	Quarantine - Automatically Quarantine New Clients - Windows XP / Server 2003	<Unspecified>	BigFix Cli
2008	Quarantine - Quarantine Needed - Windows 2000	<Unspecified>	BigFix Cli
2017	Quarantine - Quarantine Needed - Windows Vista / Server 2008 / 7 / Server 2008 R2 / 8 / 8.1 / Server 2012	<Unspecified>	BigFix Cli
2007	Quarantine - Quarantine Needed - Windows XP / Server 2003	<Unspecified>	BigFix Cli
2006	Quarantine - Quarantine No Longer Needed - Windows 2000	<Unspecified>	BigFix Cli
2016	Quarantine - Quarantine No Longer Needed - Windows Vista / Server 2008 / 7 / Server 2008 R2 / 8 / 8.1 / Server 2012	<Unspecified>	BigFix Cli

Fixlet: Quarantine - Quarantine Needed - Windows Vista / Server 2008 / 7 / Server 2008 R2 / 8 / 8.1 / Server 2012

Description

The listed computers have been determined to be out of compliance and are not in quarantine. The action below will place client computers in quarantine by using Windows Firewall with Advanced Security. The computer's network access will be blocked, allowing only BES traffic to go through. When taken as a policy action, the action will place a computer into quarantine whenever it is found to be out of compliance.

Note: You may want to display a message to the end user before placing the computer in quarantine by using the "Message" option in the "Take Action" dialog. Be sure to enable the option to "automatically close message box and run action after X minutes".

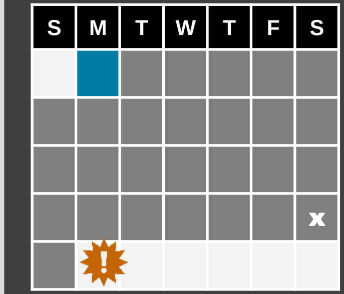
Note: If a quarantined computer is in compliance, you can remove it from quarantine using "Quarantine No Longer Needed", or deploying the "Quarantine Override" task. The current compliance and quarantine status of each client can be viewed through the "Compliance Evaluation Information" analysis.

Note: The quarantine action will allow TCP and UDP traffic on the BES Listen Port, and DNS queries, which are necessary for communication with the BES Server.

Connected to 'bigfixserver' as user 'Admin'

IBM Threat Protection System:

- ● Prevent
- ● Detect
- ○ Respond



Attack Chain Stage:

Break-In

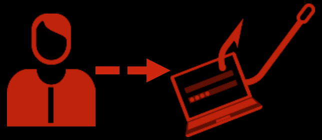
Latch-on

Expand

Gather

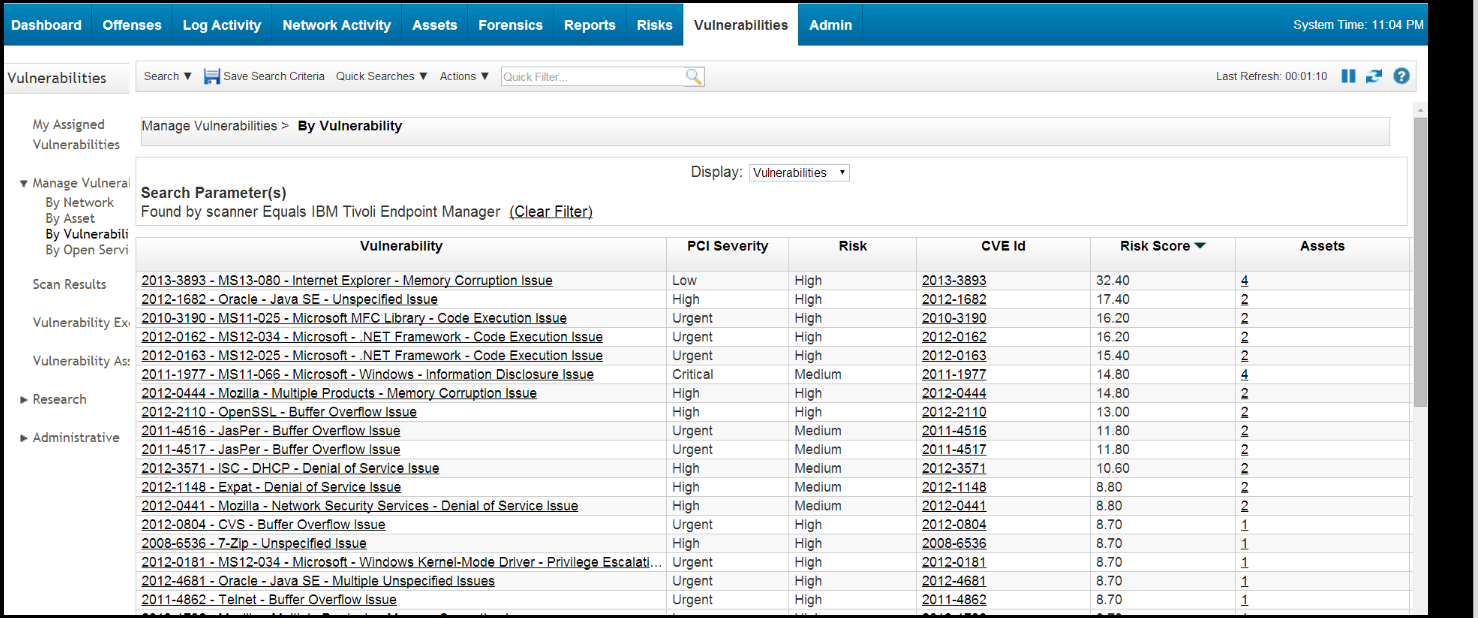
Exfiltrate

29 days earlier



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

The malware attempts to take advantage of an existing vulnerability but IBM Endpoint Manager applies patches and adjusts configuration settings to eliminate the vulnerability and reports the vulnerability to QRadar in for further analysis



Manage Vulnerabilities > **By Vulnerability**

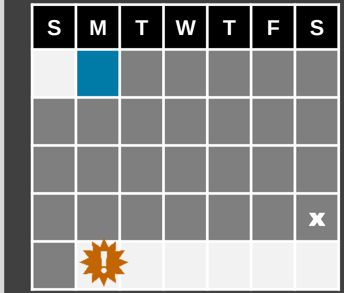
Display: Vulnerabilities ▾

Search Parameter(s)
Found by scanner Equals IBM Tivoli Endpoint Manager (Clear Filter)

Vulnerability	PCI Severity	Risk	CVE Id	Risk Score ▼	Assets
2013-3893 - MS13-080 - Internet Explorer - Memory Corruption Issue	Low	High	2013-3893	32.40	4
2012-1682 - Oracle - Java SE - Unspecified Issue	High	High	2012-1682	17.40	2
2010-3190 - MS11-025 - Microsoft MFC Library - Code Execution Issue	Urgent	High	2010-3190	16.20	2
2012-0162 - MS12-034 - Microsoft - .NET Framework - Code Execution Issue	Urgent	High	2012-0162	16.20	2
2012-0163 - MS12-025 - Microsoft - .NET Framework - Code Execution Issue	Urgent	High	2012-0163	15.40	2
2011-1977 - MS11-066 - Microsoft - Windows - Information Disclosure Issue	Critical	Medium	2011-1977	14.80	4
2012-0444 - Mozilla - Multiple Products - Memory Corruption Issue	High	High	2012-0444	14.80	2
2012-2110 - OpenSSL - Buffer Overflow Issue	High	High	2012-2110	13.00	2
2011-4516 - JasPer - Buffer Overflow Issue	Urgent	Medium	2011-4516	11.80	2
2011-4517 - JasPer - Buffer Overflow Issue	Urgent	Medium	2011-4517	11.80	2
2012-3571 - ISC - DHCP - Denial of Service Issue	High	Medium	2012-3571	10.60	2
2012-1148 - Expat - Denial of Service Issue	High	Medium	2012-1148	8.80	2
2012-0441 - Mozilla - Network Security Services - Denial of Service Issue	High	Medium	2012-0441	8.80	2
2012-0804 - CVS - Buffer Overflow Issue	Urgent	High	2012-0804	8.70	1
2008-6536 - 7-Zip - Unspecified Issue	High	High	2008-6536	8.70	1
2012-0181 - MS12-034 - Microsoft - Windows Kernel-Mode Driver - Privilege Escalati...	Urgent	High	2012-0181	8.70	1
2012-4681 - Oracle - Java SE - Multiple Unspecified Issues	Urgent	High	2012-4681	8.70	1
2011-4862 - Telnet - Buffer Overflow Issue	Urgent	High	2011-4862	8.70	1

IBM Threat Protection System:

- ● Prevent
- ● Detect
- ○ Respond



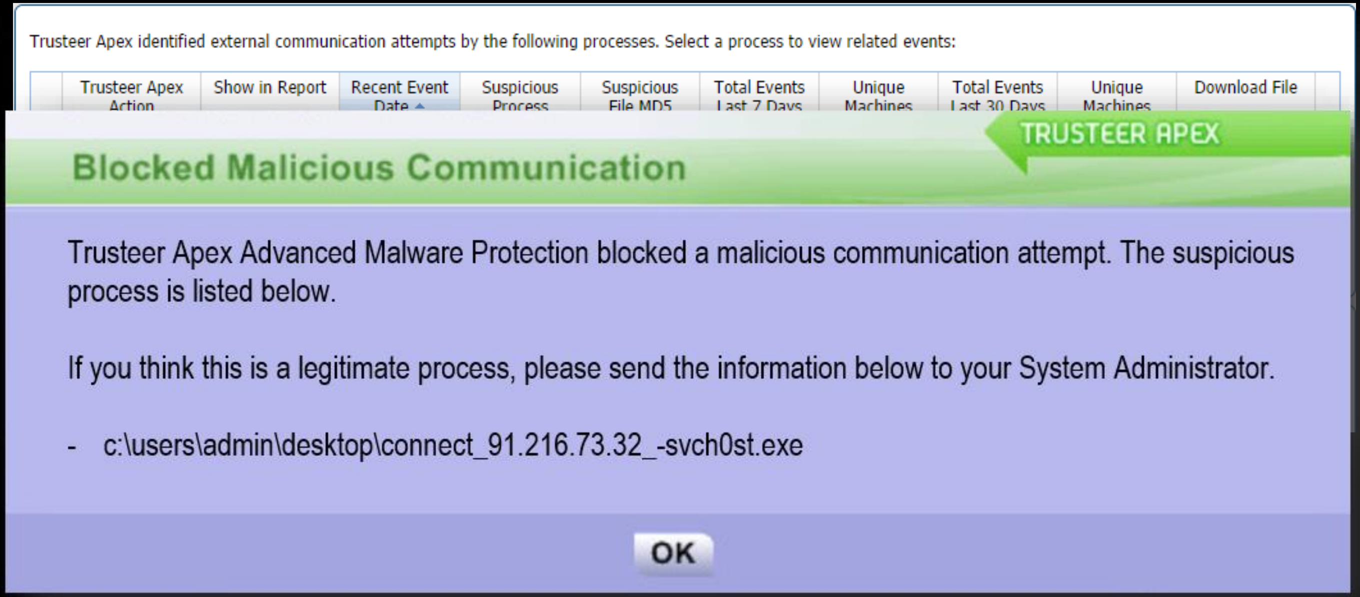
Attack Chain Stage:

- **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



Trusteer Apex identified external communication attempts by the following processes. Select a process to view related events:

Trusteer Apex Action	Show in Report	Recent Event Date ▲	Suspicious Process	Suspicious File MD5	Total Events Last 7 Days	Unique Machines	Total Events Last 30 Days	Unique Machines	Download File

Blocked Malicious Communication

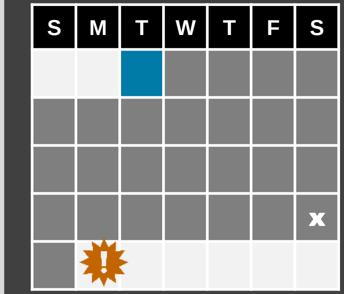
Trusteer Apex Advanced Malware Protection blocked a malicious communication attempt. The suspicious process is listed below.

If you think this is a legitimate process, please send the information below to your System Administrator.

- c:\users\admin\desktop\connect_91.216.73.32_-svch0st.exe

IBM Threat Protection System:

- ● Prevent
- ○ Detect
- ○ Respond



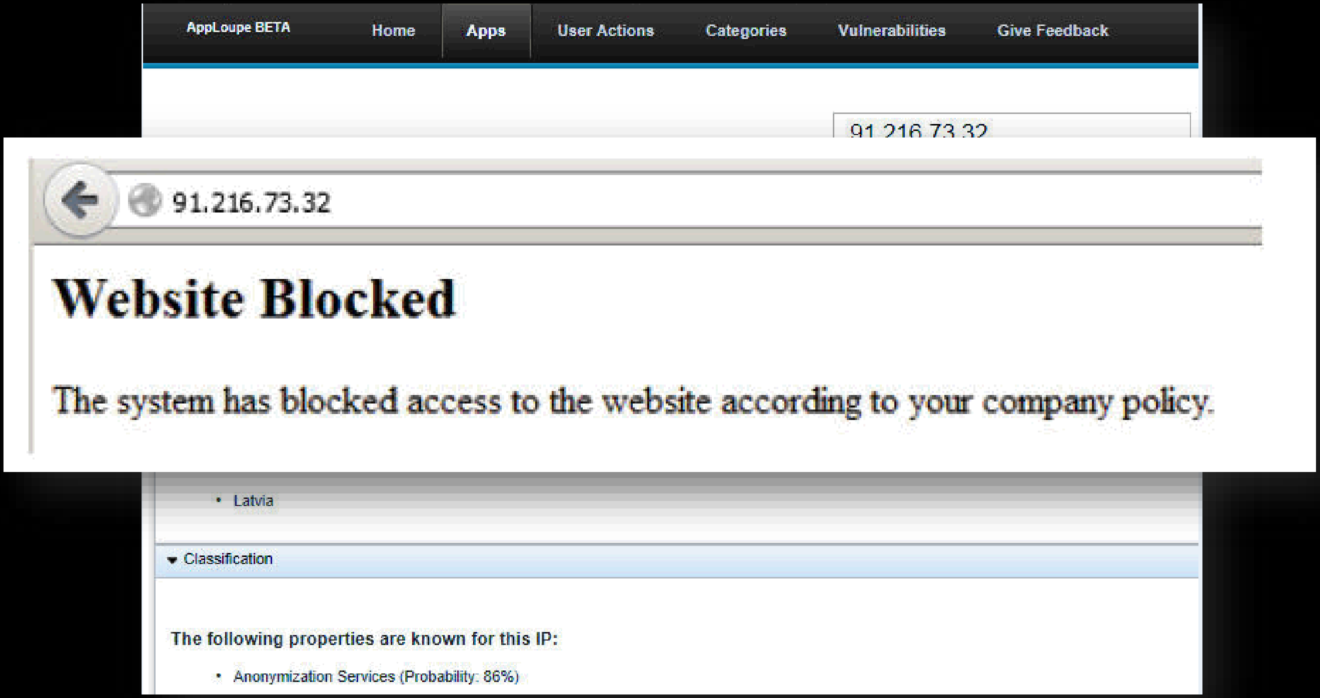
Attack Chain Stage:

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

28 days earlier

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

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



91.216.73.32

91.216.73.32

Website Blocked

The system has blocked access to the website according to your company policy.

- Latvia

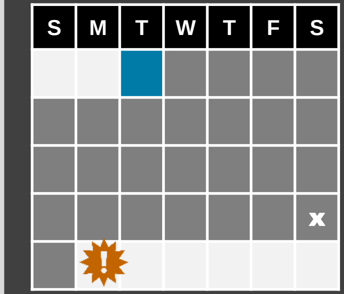
Classification

The following properties are known for this IP:

- Anonymization Services (Probability: 86%)

IBM Threat Protection System:

● Prevent
○ Detect
○ Respond



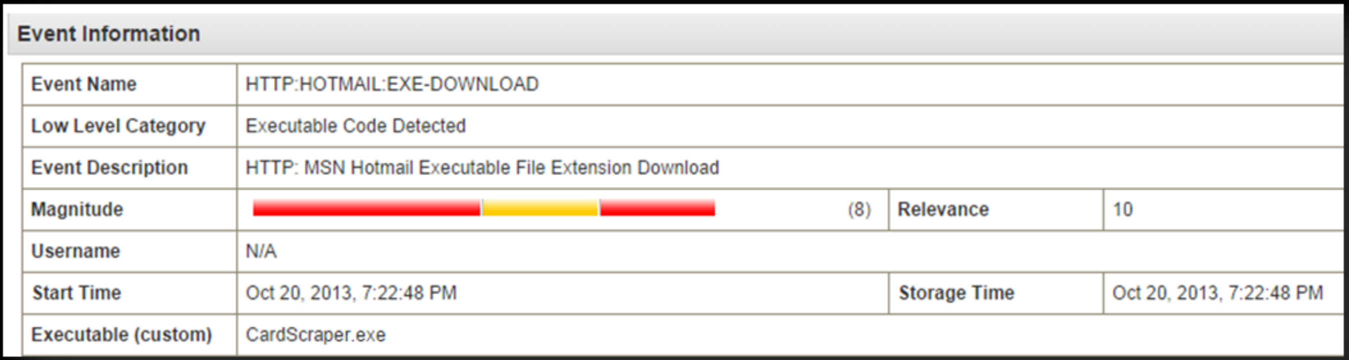
Attack Chain Stage:

- 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

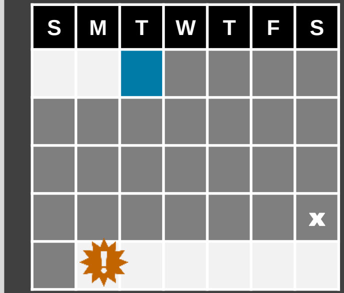


Event Information

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



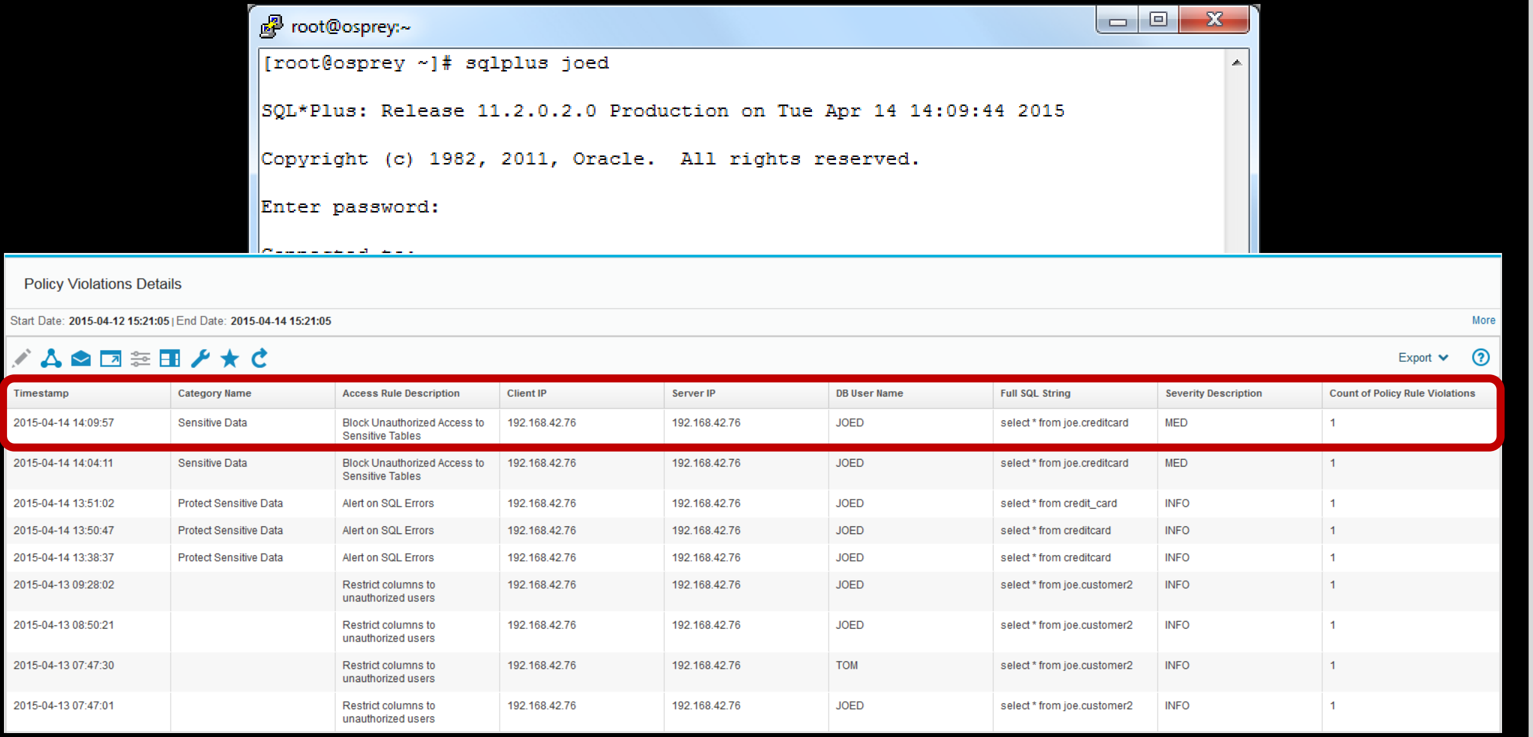
Attack Chain Stage:

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

2-3 weeks earlier

CardScraper.exe is copied to POS servers throughout the business

IBM Guardium Data Activity Monitor blocks the unauthorized connection to the database servers.



```
[root@osprey ~]# sqlplus joed

SQL*Plus: Release 11.2.0.2.0 Production on Tue Apr 14 14:09:44 2015

Copyright (c) 1982, 2011, Oracle.  All rights reserved.

Enter password:

Connected to:
```

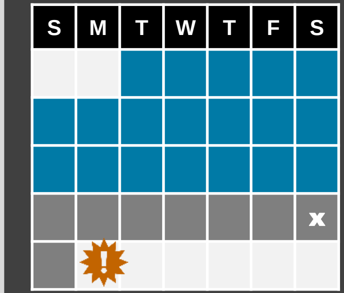
Policy Violations Details

Start Date: **2015-04-12 15:21:05** | End Date: **2015-04-14 15:21:05**

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Count of Policy Rule Violations
2015-04-14 14:09:57	Sensitive Data	Block Unauthorized Access to Sensitive Tables	192.168.42.76	192.168.42.76	JOED	select * from joe.creditcard	MED	1
2015-04-14 14:04:11	Sensitive Data	Block Unauthorized Access to Sensitive Tables	192.168.42.76	192.168.42.76	JOED	select * from joe.creditcard	MED	1
2015-04-14 13:51:02	Protect Sensitive Data	Alert on SQL Errors	192.168.42.76	192.168.42.76	JOED	select * from credit_card	INFO	1
2015-04-14 13:50:47	Protect Sensitive Data	Alert on SQL Errors	192.168.42.76	192.168.42.76	JOED	select * from creditcard	INFO	1
2015-04-14 13:38:37	Protect Sensitive Data	Alert on SQL Errors	192.168.42.76	192.168.42.76	JOED	select * from creditcard	INFO	1
2015-04-13 09:28:02		Restrict columns to unauthorized users	192.168.42.76	192.168.42.76	JOED	select * from joe.customer2	INFO	1
2015-04-13 08:50:21		Restrict columns to unauthorized users	192.168.42.76	192.168.42.76	JOED	select * from joe.customer2	INFO	1
2015-04-13 07:47:30		Restrict columns to unauthorized users	192.168.42.76	192.168.42.76	TOM	select * from joe.customer2	INFO	1
2015-04-13 07:47:01		Restrict columns to unauthorized users	192.168.42.76	192.168.42.76	JOED	select * from joe.customer2	INFO	1

IBM Threat Protection System:

- ● Prevent
- ○ Detect
- ○ Respond



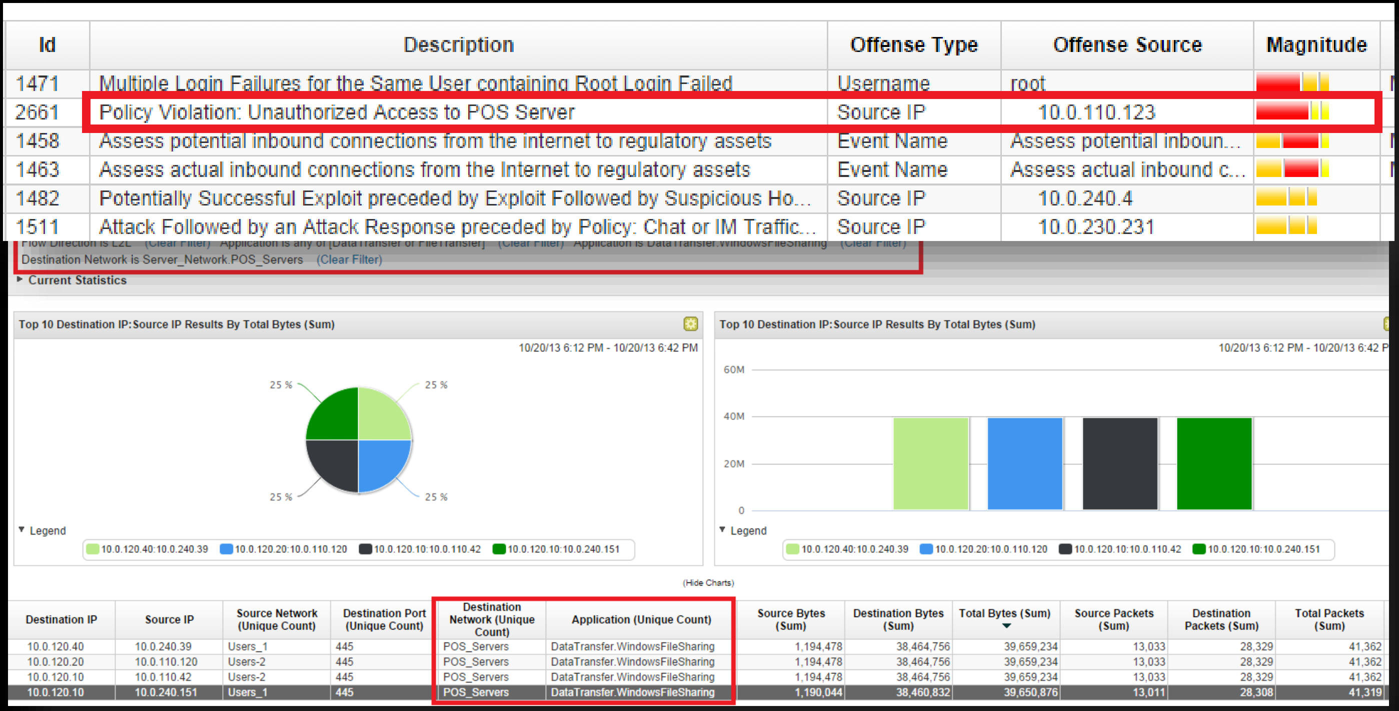
Attack Chain Stage:

- 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	

Flow Direction is L2L (Clear Filter) Application is any of [DataTransfer or FileTransfer] (Clear Filter) Application is DataTransfer.WindowsFileSharing (Clear Filter)
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

▾ 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 P

▾ Legend

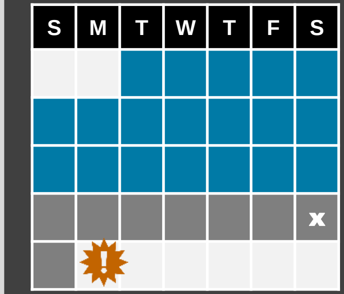
🟩 10.0.120.40:10.0.240.39 🟦 10.0.120.20:10.0.110.120 ⬛ 10.0.120.10:10.0.110.42 🟩 10.0.120.10:10.0.240.151

(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

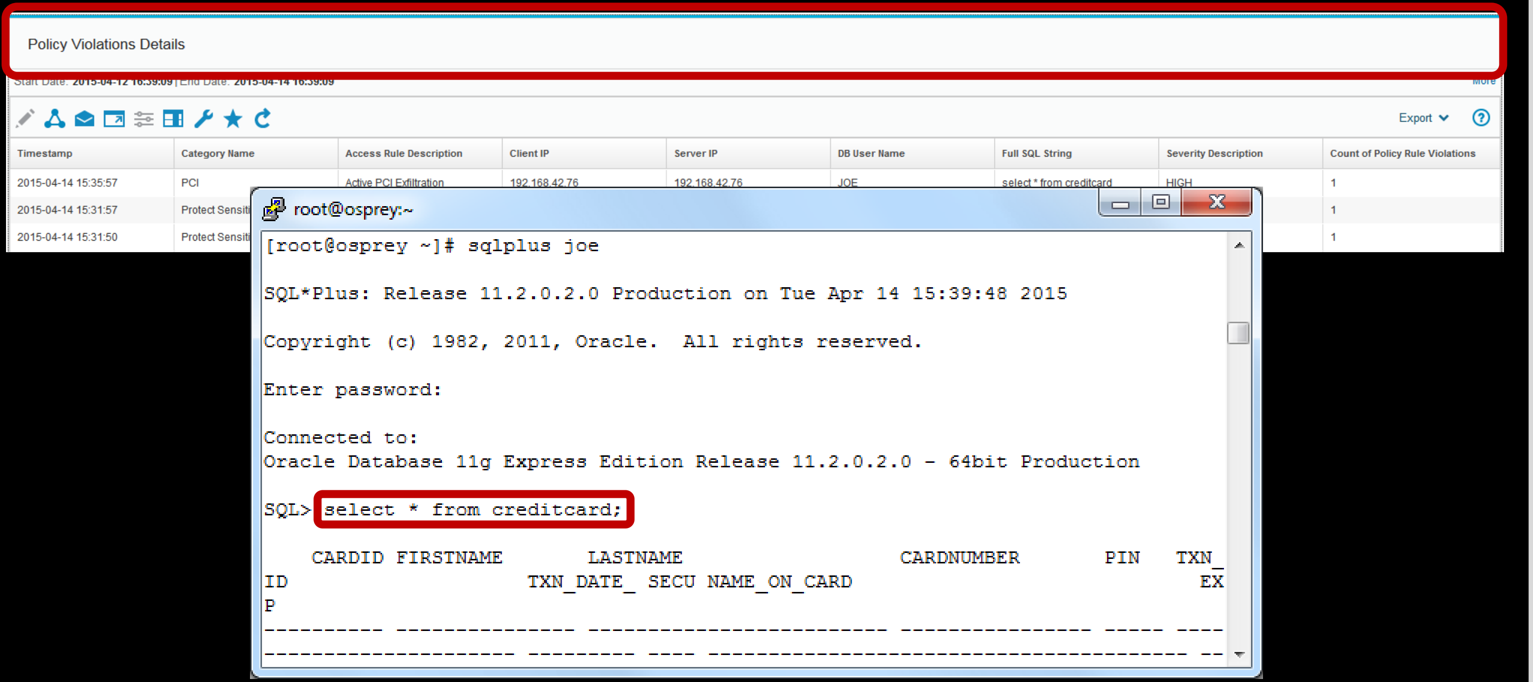
Gather

Exfiltrate

The previous week

PCI was transferred from infected POS servers to a single server

IBM Guardium Data Activity Monitor alerts on the suspicious activity of the attempt by an unauthorized user to access a large amount of sensitive data as a potential precursor to an exfiltration attempt, raising the offense to IBM QRadar SIEM



Policy Violations Details

Start Date: 2015-04-12 16:39:09 | End Date: 2015-04-14 16:39:09

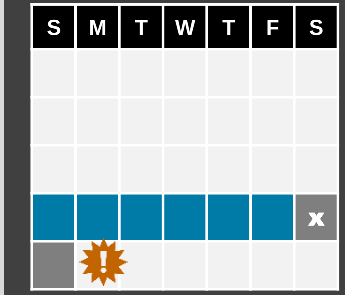
Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Count of Policy Rule Violations
2015-04-14 15:35:57	PCI	Active PCI Exfiltration	192.168.42.76	192.168.42.76	JOE	select * from creditcard	HIGH	1
2015-04-14 15:31:57	Protect Sensiti							1
2015-04-14 15:31:50	Protect Sensiti							1

root@osprey:~

```
[root@osprey ~]# sqlplus joe

SQL*Plus: Release 11.2.0.2.0 Production on Tue Apr 14 15:39:48 2015

Copyright (c) 1982, 2011, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL> select * from creditcard;

    CARDID FIRSTNAME       LASTNAME                  CARDNUMBER       PIN   TXN_
ID                     TXN_DATE_ SECU NAME_ON_CARD                        EX
P
---------- --------------- ------------------------- ---------------- ----- ----
-------------------- --------- ---- ---------------------------------------- --
```

IBM Threat Protection System:

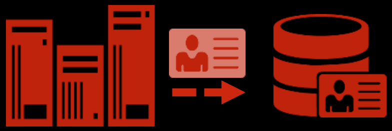
- Prevent
- Detect
- Respond



Attack Chain Stage:

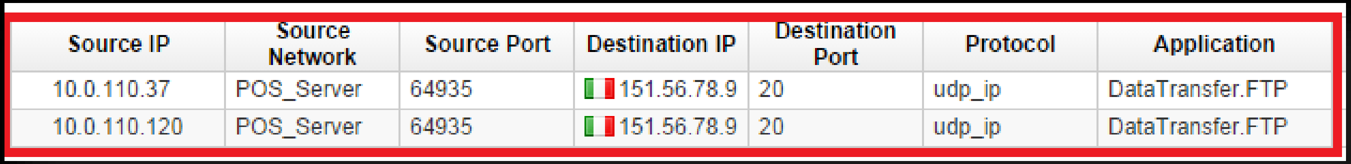
- Break-In
- Latch-on
- Expand
- **Gather**
- Exfiltrate

The previous week



PCI was transferred from infected POS servers to a single server

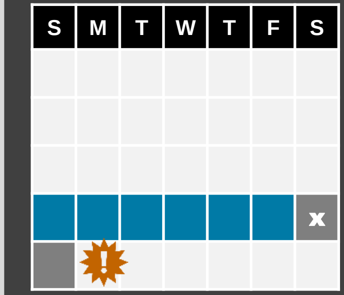
IBM QRadar SIEM detects communication behavior that deviates from corporate and compliance policies



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:

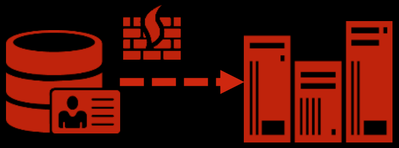
○ Prevent
● Detect
○ Respond



Attack Chain Stage:

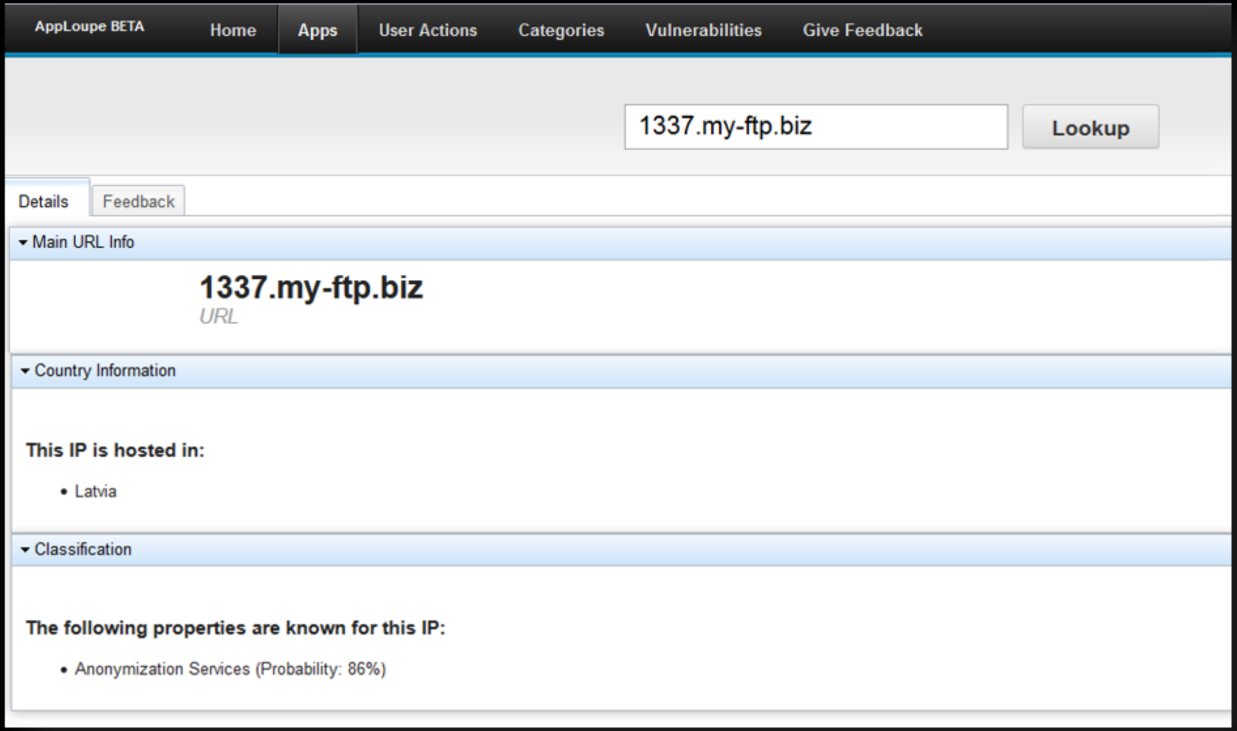
- Break-In
- Latch-on
- Expand
- Gather
- Exfiltrate

The previous Saturday



A server connects to an unknown external FTP server and the PCI 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”



1337.my-ftp.biz

▾ Main URL Info

1337.my-ftp.biz
URL

▾ Country Information

This IP is hosted in:

- Latvia

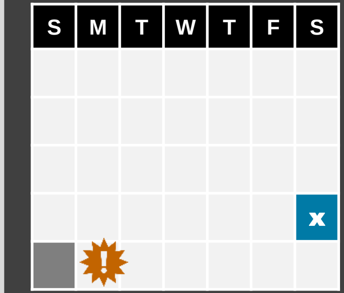
▾ Classification

The following properties are known for this IP:

- Anonymization Services (Probability: 86%)

IBM Threat Protection System:

◉ Prevent
● Detect
● Respond



Attack Chain Stage:

Break-In

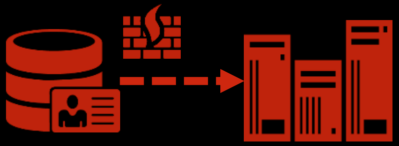
Latch-on

Expand

Gather

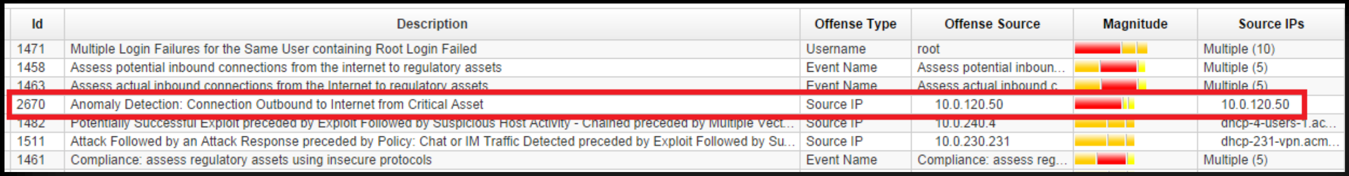
Exfiltrate

The previous Saturday

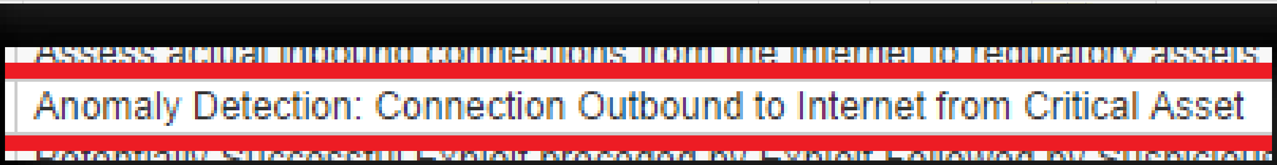


A server connects to an unknown external FTP server and the PCI is exfiltrated.

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)



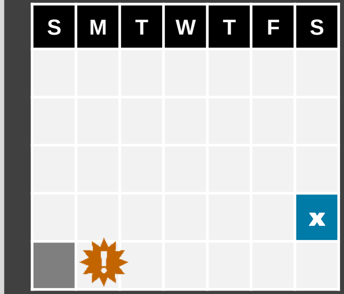
Anomaly Detection: Connection Outbound to Internet from Critical Asset

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…

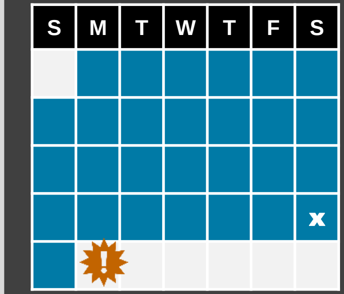
- Query external server addresses found on the underground forum
- Report internal connections
- Show external file transfers
- Identify malware transferred by the attacker
- Discover connection histories and extended relationships with internal assets and identities

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 critical

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

IBM offers Emergency Response Services to help.

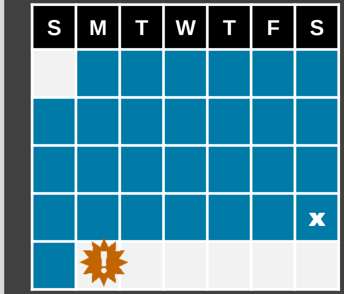
Cyber Emergency Hotline

(US) 1-888-241-9812
(Worldwide) 1-312-212-8034

- **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

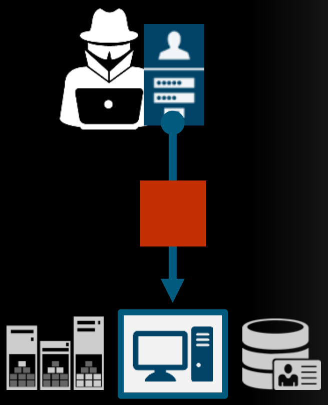
Latch-on

Expand

Gather

Exfiltrate

A dynamic, integrated system to help break the attack chain.



1. Break-in
2. Latch-on
3. Expand
4. Gather
5. Exfiltrate

Focus on critical points in the attack chain with preemptive defenses on endpoints, the network, and critical data repositories.

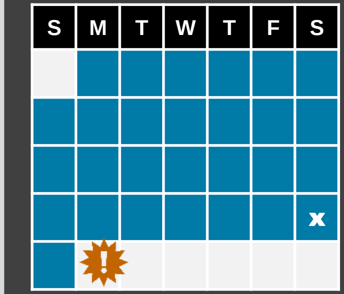
Continuously monitor activity from across the entire organization.

Rapidly investigate breaches, retrace activity, and learn from findings.

Prevent. Detect. Respond.

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

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.