Data Breach Digest

Perspective is Reality.

verizon✓

Table of Contents

The Situation Room

Data breaches are complex affairs often involving some combination of human factors, hardware devices, exploited configurations or malicious software. As can be expected, data breach response activities — investigation, containment, eradication, notification, and recovery — are proportionately complex.

These response activities, and the lingering post-breach aftereffects, aren't just an IT security problem; they're an enterprise problem involving Legal Counsel, Human Resources, Corporate Communications and other Incident Response (IR) stakeholders. Each of these stakeholders brings a slightly different perspective to the breach response effort.

Last year, thousands of IR and cybersecurity professionals delved into the inaugural "Data Breach Digest — Scenarios from the Field" (aka "the RISK Team Ride-Along Edition") to get a first-hand look into the inner workings of data breaches from an investigative response point of view (PoV).

Continued research into our recent caseload still supports our initial inklings that just over a dozen or so prevalent scenarios occur at any given time. Carrying forward from last year, we have come to realize that these data breach scenarios aren't so much about threat actors, or even about the vulnerabilities they exploited, but are more about the situations in which the victim organizations and their IR stakeholders find themselves. This gives each scenario a distinct personality ... a unique persona, per se.

This year, for the "Data Breach Digest — Perspective is Reality" (aka "the IR Stakeholder Edition"), we took a slightly different approach in bringing these scenarios to life. Each scenario narrative — again, based on real-world data breach response activities — is told from a different stakeholder PoV. As such, the PoV covers their critical decision pivot points, split-second actions taken, and crucial lessons learned from cases investigated by us – the Verizon RISK Team.

> Data breaches — and the lingering post-breach aftereffects — aren't just an IT security problem: they're an enterprise problem.

These scenarios draw from real-world cybersecurity incident investigations. To protect victim anonymity, we modified certain details and took some creative license in writing the scenario narratives. This included, but wasn't limited to, changing names, geographic locations, and other details, such as the quantity of records stolen, and monetary loss details.

> Each scenario narrative ... is told from a different stakeholder PoV. As such, the PoV covers critical decision pivot points, split-second actions taken, and crucial lessons learned.

With this "Perspective is Reality" edition, readers can put themselves in the shoes of various IR stakeholders and in doing so, formulate or improve countermeasures to improve their cybersecurity incident mitigation and response efforts.

Welcome to the Situation Room!

DBD Components

Before we talk about its components, it is worth mentioning what the Data Breach Digest (DBD) is. Probably the best way to describe the DBD is that it's a companion to the annual Data Breach Investigations Report (DBIR). The DBIR is our annual publication on security. It is chock-full of statistics, metrics and insight into the who, what, where, when and how of data breaches and cybersecurity incidents.

The DBD is the DBIR's alter ego – it complements and supplements the DBIR by bringing data breaches to life through narratives told by breach responders. It's light on metrics, but heavy on experiences. So use the DBIR to frame your argument for enterprise change; use the DBD to illustrate why such change is needed.

Now that we have that out of the way, let's talk about the components that make up the DBD: the victim industries, the incident patterns, the breach scenarios, and finally, we'll introduce you to the IR stakeholders.

Victim industries

As with the DBIR, we used the North American Industry Classification System (NAICS) for the coding of the 12 most relevant victim industries in the DBD based on our VERIS dataset.[1]

Incident patterns

Some scary numbers come from our incident data set (now 12 years old). Hundreds of thousands of cybersecurity incidents and thousands of confirmed data breaches paint a bleak picture – no happy clouds or trees here. The good news is that we don't have to worry about thousands of unique attack types when defending your data, and by extension, your business. There are recurring combinations of actors, actions, assets and attributes, which provide us a scouting report on what comprises an incident.

> Use the DBIR to frame your argument for enterprise change; use the DBD to illustrate why such change is needed.

According to the 2016 DBIR, over 90% of data breaches fell into one of nine incident patterns. Some patterns are everybody's problems (e.g., Crimeware, Physical theft and loss) and some aren't relevant to all organizations (e.g., Payment card skimmers). Knowing which incident patterns affect your industry more often than others do provides a solid building block for allocating cybersecurity resources.

A brief refresher on VERIS

Whenever we delve into our caseload and write statements about "how many" or "how often," we rely on the VERIS (Vocabulary for Event Recording and Incident Sharing) Framework. VERIS serves a common contextual database answering the "who" (threat actors), "what" (victim assets), "why" (threat motives), and "how" (threat actions) for previously collected cybersecurity incident and data breach content. In short, VERIS provides a common language for describing security incidents in a structured and repeatable manner.

Incorporating VERIS into your IR Plan empowers you to collect and track your own incident data and compare your data to that of other contributors. This data allows you to conduct in-house analysis of what types of incidents, historically, have caused you the most agitation and drive projects to reduce your exposure to those incidents. After the fact, VERIS can provide objective metrics to compare your incident data and see if there is any measurable improvement.

And yes, since VERIS is community-supported, it's free (yep, free) for any and all to use. More details can be found here: www.veriscommunity.net.

---

1   http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2017'

> Knowing which incident patterns affect your industry more often than others do provides a building block for allocating cybersecurity resources.

These nine incident patterns are as follows:

1. **Insider and privilege misuse –** trusted actors leveraging logical and/or physical access in an inappropriate or malicious manner.

2. **Cyber-espionage –** targeted attacks from external actors hunting for sensitive internal data and trade secrets.

3. **Web application attacks –** web-application-related stolen credentials or vulnerability exploits.

4. **Crimeware –** malware incidents, typically opportunistic and financially motivated in nature (e.g., banking Trojans, ransomware).

5. **Point-of-sale (POS) Intrusions –** attacks on POS environments leading to payment card data disclosure.

6. **Denial of service (DoS) Attacks –** non-breach-related attacks affecting business operations.

7. **Payment card skimmers –** physical tampering of ATMs and fuel-pump terminals.

8. **Physical theft and loss –** physical loss or theft of data or IT-related assets.

9. **Miscellaneous errors –** an error directly causing data loss.

Of the nine DBIR incident patterns, we chose six for this year's DBD, five of which are directly related to data breaches. Although not typically considered a data breach, we included DoS attacks as the sixth incident pattern. Three incident patterns weren't included for the following reasons: 7 – Payment card skimmers (physical threat, not typically investigated by us), 8 – Physical theft and loss (physical threat, not usually investigated by us), and 9 – Miscellaneous errors (mistakes, no malicious threat actors).

Data breach scenarios

For ease of use, we once again divvied up the data breach scenarios into four "clustered groupings:"

1. The Human Element – four scenarios highlighting human-related threat actors or targeted victims.

2. Conduit Devices – four scenarios covering device misuse or tampering.

3. Configuration Exploitation – four scenarios focusing on reconfigured or misconfigured settings.

4. Malicious Software – four scenarios centering on sophisticated or special-purpose illicit software.

If you're confused between "breach scenarios" and "incident patterns," the basic difference is that the data breach scenarios are specific examples that fall under one of the six chosen incident patterns.

> Of the nine DBIR incident patterns, we chose six for this year's DBD. Although not typically considered a data breach, this year we included DoS attacks as the sixth incident pattern.

Similar to last year's DBD, we categorized each scenario in one of two ways: "prevalent" or "lethal." The "prevalent" scenarios are those we have seen most frequently (e.g., a threat actor's most likely course of action). The "lethal" scenarios are those we have seen less frequently, but consider most destructive (e.g., a threat actor's most dangerous course of action). Of the 16 scenarios, we identified ten as the most prevalent and six as the most lethal.

This year we came up with nine new data breach scenarios and rounded these out with seven scenarios from last year. All scenarios have brand new narratives, and yes, there are 16 fresh "scenari-catures" (scenario caricatures). The 16 data breach scenarios, broken down by "clustered groupings", are shown on page 6.

"Scenario" to "clustered group" mapping

Clustered Grouping	Scenario Number	Scenario Name	Scenari-cature	Occurence
The Human Element	HE-1	Financial Pretexting	the Golden Fleece	Prevalent
	HE-2	Hactivist Attack	the Epluribus Enum	Lethal
	HE-3	Partner Misuse	the Indignant Mole	Lethal
	HE-4	Disgruntled Employee	the Absolute Zero	Prevalent
Conduit Devices	CD-1	C2 Takeover	the Broken Arrow	Prevalent
	CD-2	Mobile Assault	the Secret Squirrel	Lethal
	CD-3	IoT Calamity	the Panda Monium	Lethal
	CD-4	USB Infection	the Hot Tamale	Prevalent
Configuration Exploitation	CE-1	Website Defacement	the Hedley Kow	Prevalent
	CE-2	DDoS Attack	the 12000 Monkeyz	Lethal
	CE-3	ICS Onslaught	the Fiddling Nero	Lethal
	CE-4	Cloud Storming	the Acumulus Datum	Prevalent
Malicious Software	MS-1	Crypto Malware	the Fetid Cheez	Prevalent
	MS-2	Sophisticated Malware	the Pit Viper	Prevalent
	MS-3	RAM Scraping	the Bare Claw	Prevalent
	MS-4	Unknown Unknowns	the Polar Vortex	Prevalent

Where are they now?

We've carried over seven data breach scenarios from last year's 18 scenarios. These carry-over scenarios consisted of "Financial Pretexting" (formerly "the Slick Willie"), "Hacktivist Attack" (formerly "the Dark Shadow"), "Partner Misuse" (formerly "the Busted Chain"), "USB Infection" (formerly "the Porta Bella"), "Data Ransomware" (formerly "the Catch 22"), "Sophisticated Malware" (formerly "the Flea Flicker"), and "RAM Scraping" (formerly "the Leaky Boot"). Our reason for carrying over these scenarios? Their sheer prevalence and/or continued lethality.

As for the other eleven scenarios that we didn't carry over? As much as we hate to see "the Roman Holiday" scenari-cature not roll out for another year, we had to move on from him and his other scenari-cature compatriots. These scenarios didn't make the cut for one or more reasons: they're lethal, but not very prevalent (we brought this to your attention already, why repeat), they're an element of another scenario (e.g., "Social Engineering" factors into many of this year's scenarios), they're a subset of another scenario (e.g., "Disgruntled Employee" is a subset of the "Insider Threat"), or they just weren't seen much in this year's caseload (e.g., "Peripheral Tampering").

Incident response stakeholders

In our many years of investigative response experience, we have seen IR stakeholders come in all shapes and sizes, and vary in numbers too – from one to dozens to many more. One way to look at IR stakeholders is to consider them as "technical" and "non-technical" stakeholders (remember data breaches aren't just an IT security problem). However, perhaps the best (and most useful) way is to characterize IR stakeholders by their roles and responsibilities, and in some cases, their authorities.

If we look further into the types of IR stakeholders, we see they often include top-level leadership (the "strategic" decision-makers), middle-level managers (the "tactical" decision-makers), and a veritable cornucopia of technical and non-technical subject matter experts on cybersecurity incident and data breach response.

If we organized these stakeholders not by specialty, but by relationship to the victim organization, we have two groups: "internal" stakeholders – those who are part of the victim organization, and "external" stakeholders – those who are outside the victim organization.

For this year's scenario narrators, we feature 16 different stakeholders to present a data breach scenario from their respective PoV while focusing on those items most important to their roles and responsibilities. For the DBD scenario internal (a.k.a. victim) stakeholders, we selected ten PoVs, and for the DBD scenario external stakeholders, we chose six RISK Team PoVs.

Internal stakeholders

Stakeholder PoV	Scenario Name	Scenari-cature
CIO	Financial Pretexting	Responsible for enterprise IT strategy, networks, systems, and applications for an organization
CISO	Crypto Malware	Manages information security implications from strategic goals to personnel to infrastructure to policy to cybersecurity activities
Legal Counsel	Partner Misuse	Provides legal advice and recommendations on cybersecurity incidents and response activities
Human Resources	Disgruntled Employee	Provides guidance and assistance for cybersecurity incidents involving employee activity or employee Personally Identifiable Information (PII) related breaches
Corporate Comms	Website Defacement	Manages internal and external communications related to cybersecurity incidents
Incident Commander	IoT Calamity	Leads the tactical IR Team by providing direction and guidance; represents the tactical IR Team during stakeholder meetings; updates stakeholders on response progress
Internal Investigator	USB Infection	Conducts investigations into allegations of employee misconduct
IT Security Manager	Cloud Storming	Manages IT Team and IT security aspects (e.g., applications, systems, network)
SOC Analyst	DDoS Attack	Monitors for and initially responds to cybersecurity incidents
EDR Technician	Unknown Unknowns	Manages and leverages response capability of Endpoint Detection and Response (EDR) tool

External stakeholders - The RISK Team

Stakeholder PoV	Scenario Name	Scenari-cature
Lead Investigator	Hacktivist Attack	Runs the digital forensics investigation; serves as the primary point of contact for the victim organization
Endpoint Forensics Examiner	Mobile Assault	Examines endpoint systems, to include disk and physical memory artifacts
Malware Reverse Engineer	Sophisticated Malware	Analyzes malicious software (malware) through malware reverse engineering
Network Forensics Specialist	C2 Takeover	Examines network-related data sources, to include packet captures, NetFlow data, and network logs and device configurations
CIP/CS Specialist	ICS Onslaught	Assesses Industrial Critical Infrastructure Protection (CIP)
PFI Investigator	RAM Scraping	Conducts Payment Card Industry (PCI) forensic investigations

The Verizon RISK Team

The RISK Team performs cybersecurity investigations for hundreds of commercial enterprises and government agencies annually across the globe. Over the previous three years, we conducted over 1,400 engagements for our customers.

For conducting investigative response engagements, our skillsets include endpoint forensics, malware reverse engineering, network forensics, mobile device forensics, complex data recovery, critical infrastructure protection/cybersecurity assessments, PCI forensic investigations, darknet research, among others.

Our investigative expertise and well-seasoned experience are encapsulated in the annual DBIR and its companion — this publication — the DBD.

Using the DBD

We wrote the DBD with the intent that folks read it from front to back (and perhaps even repeatedly afterwards). Of course, that's our hope, but we realize folks are pressed for time, so we constructed the DBD in such a way that they can zero in on certain areas (save time now, and save the rest of the DBD for later). So, here are your DBD usage options:

1. Dive in and read from start to finish (takes time, but you get the full 360 degree perspective).

2. Hone in on a specific Clustered Grouping (focuses your reading pleasure to related scenarios).

3. Take a targeted approach and use the handy-dandy DBD Usage Matrix on the next page that walks you through a three-step process (1 – victim industry 2 – incident pattern 3 – relevant breach scenario) to identify the most applicable scenario(s) to you.

And don't forget, if you choose an option other than Option #1, when you do have the time, come back to the DBD and read the rest of the scenarios for a more well-rounded perspective!

Finding the scenarios most relevant to you and your organization is made easy by using "the DBD Usage Matrix." The DBD usage matrix consists of the previously discussed DBD Components: Victim industries, incident patterns and relevant scenarios.

To use the DBD Usage Matrix, on page 10, follow these three steps:

1. **Victim industry.** Start with the left column "Victim industry," move down, and select your industry.

2. **Incident pattern.** Then, go up to the header "Incident pattern," move right, and select the of-interest incident pattern(s).

3. **Relevant breach scenario.** Finally, drop further down to "Relevant breach scenario," and identify the most relevant scenarios to your industry by their designated scenario by number.

DBD usage matrix incident pattern percentages

The percentages in the DBD usage matrix (page 10), are based on overall VERIS metrics for incident patterns by NAICS industry with a minimum of 25 cybersecurity incidents over the previous year. The "gold" boxes (Danger, Will Robinson!) are those percentages at/above 5%, the "orange" boxes (put down the pizza and soda and check this out) are those at/above 15%, and the "red" boxes (Houston, we have a problem) are those at/above 25%.

In the DBD usage matrix, the "victim industry" x "incident pattern" percentages were drawn from DBIR 2016 "Figure 21. Incident patterns by industry, minimum 25 incidents."

The DBD usage matrix

1 – Victim industry (NAICS #)[2] ▼	2 – Incident pattern ▼					
	Insider and privilege misuse	Cyber-espionage	Web application attacks	Crimeware	POS intrusions	DoS attacks
Accommodation and Food Services (72)	2%	<1%	1%	<1%	74%	20%
Administrative and Support … (56)	22%		11%		4%	56%
Educational Services (61)	1%	2%	5%	2%		81%
Arts, Entertainment, and Recreation (71)			1%		1%	99%
Financial and Insurance (52)	3%	<1%	48%	2%	<1%	34%
Health Care and Social Assistance (62)	23%	2%	4%	4%	5%	
Information (51)	2%	3%	12%	4%	<1%	46%
Manufacturing (31-33)	6%	16%	6%	5%	1%	46%
Professional, Scientific, and Technical Services (54)	2%	2%	1%	1%		90%
Public Administration (92)	22%	<1%	<1%	16%	<1%	1%
Retail Trade (44-45)	1%	<1%	13%	1%	32%	45%
Transportation and Warehousing (48-49)	6%	16%	35%	10%		26%
3 – Relevant breach scenario ▶	▼	▼	▼	▼	▼	▼
The Human Element	HE-1 HE-2 HE-3 HE-4	HE-4				
Conduit Devices		CD-1 CD-3 CD-4		CD-1 CD-3 CD-4		CD-2 CD-3
Configuration Exploitation			CE-1 CE-4	CE-3	CE-4	CE-2
Malicious Software		MS-2 MS-4		MS-1 MS-2 MS-4	MS-3	

Attack-defend cards

> Each Attack-Defend Card is specific to the scenario and covers four areas: "breach scenario," "incident pattern," "threat actor," and "targeted victim."

For each data breach scenario, we provide an "Attack-Defend Card" along with a detailed scenario narrative. The scenarios considered "lethal" are labeled as such; those that are unlabeled are "prevalent." Each Attack-Defend Card is specific to the scenario (e.g., IoT Calamity – the Panda Monium) and covers four areas: "breach scenario," "incident pattern," "threat actor," and "targeted victim." Content is drawn from the previous three years of our RISK Team caseload, as well as other sources, including VERIS, NAICS, and Center for Inernet Security (CIS) Critical Security Controls (CSCs).

For "Key Stakeholders," see "Appendix A: Key Incident Response Stakeholders," for a listing of key IR stakeholders and their high-level responsibilities.

For "Countermeasures," see "Appendix B: CIS Critical Security Controls," for a listing of the 20 CIS CSCs.

Scenario narratives

Immediately following the Attack-Defend Card, we brought each scenario to life through a narrative walking you, the reader, from initial incident detection (and validation), to response and investigation, and then to lessons learned. And, as mentioned previously, for these 16 scenarios, each narrative is told from a different IR stakeholder PoV (e.g., CISO, SOC Analyst, PFI Investigator, etc.).

> We've brought each scenario to life through a narrative walking you, the reader, from initial incident detection (and validation), to response and investigation, and then to lessons learned.

Now sit back, settle in, enjoy the view, and gain that new perspective on data breach response!

Attack-defend card example

\<Scenario Name\> — the \<Scenari-cature\>

specific (victim), indirect (e.g., open port, application), opportunistic (e.g., phishing)

Breach scenario

Breach scenario

Sophistication level

1 — 2 — 3 — 4 — 5

1-5 based on tactics and techniques

Attributes

confidentiality, integrity, availability

Incident pattern

Pattern

most relevant incident pattern for the scenario

Time to discovery

H — D — W — M — Y

hours, days, weeks, months, years

Time to containment

H — D — W — M — Y

hours, days, weeks, months, years

Threat actor

threat actor types

Composition

espionage, financial, ideology, grudge

Motives

1-5 VERIS threat actions[4]

Tactics and techniques

Targeted victims

Industries

relevant NAICS industries[3]

Key stakeholders

key IR stakeholders

Countermeasures

CIS Critical Security Controls

high-level description of the breach scenario

The Human Element

Human beings play a significant role in data breaches and cybersecurity incidents. This should come as no surprise – after all, we are the ones who produce, consume, use, depend on, and as a result, have to secure and protect digital data. Because of this, humans fulfill the roles of threat actors, targeted victims, cybersecurity defenders and incident response stakeholders.

Looking at the VERIS data, the social threat action was used in just under one-third of confirmed data breaches, only ranking behind the VERIS threat action categories of hacking and malware in prevalence. For threat actors, those tactics and techniques used to manipulate or take advantage of victims include phishing (92%), pretexting (4%), and bribery/solicitation (3%).

As one would expect, email is the primary means of communication to the target (95%) followed by in-person deception (2%) and phone calls (2%), with a small amount of overlap across the three means of communication. Social actions are typically part of a blended attack, with a successful installation of malware or disclosure of credentials as the goal of the social phase. Social actions are usually a means to an initial foothold or a piece of information to further an attack.

Threat action varieties most attributable to human victims include social (where human assets are "compromised"), misuse (where humans under your employ are the threat actor), and error (where humans are goofing up). When we look at our VERIS data over the previous three years, we see that almost half (49%) of all breaches involve one or more of these human elements.

Scenarios HE-1 (Financial Pretexting) and HE-2 (Hacktivist Attack) focus on external threat actors with no access targeting insiders with trusted access, while Scenario HE-3 (Partner Misuse) covers a partner threat actor with some level of access, and Scenario HE-4 (Disgruntled Employee) covers a disgruntled employee with trusted access.

VERIS threat action varieties

Threat actions[5] describe what the threat actor did to cause or contribute to the incident. Every incident has at least one, but most will have multiple actions (and often across multiple categories). VERIS uses seven primary threat actions: Hacking, Malware, Social, Error, Misuse, Physical, and Environmental.
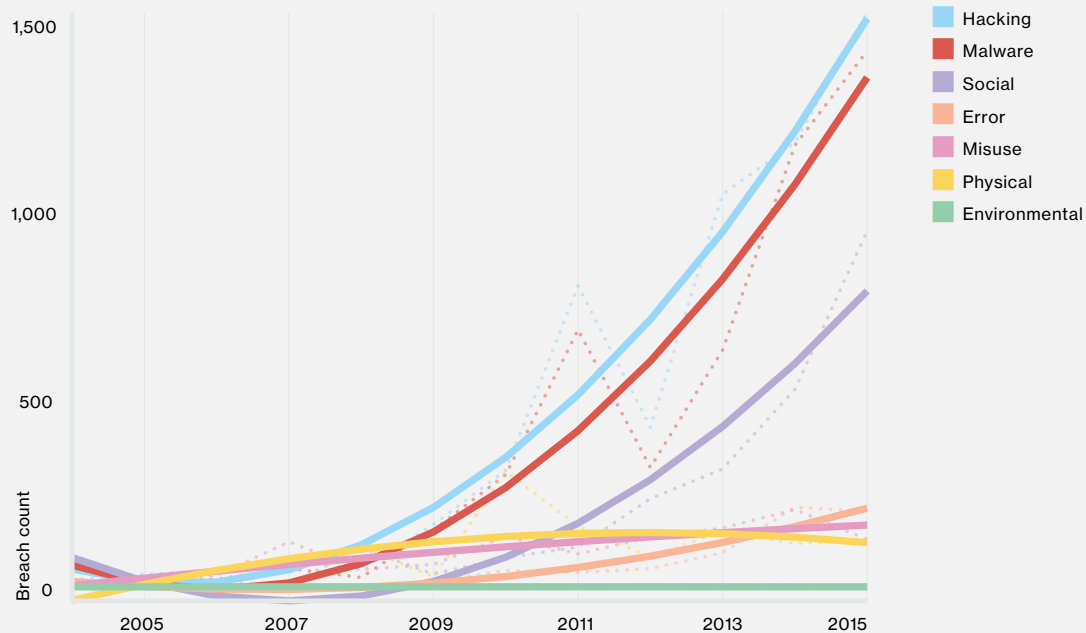
- Hacking – attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms

- Malware – any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent

- Social – deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets

- Error – broadly encompasses anything done (or left undone) incorrectly or inadvertently

- Misuse – the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended

- Physical – includes deliberate threats that involve proximity, possession, or force

- Environmental – includes natural events and hazards associated with the immediate environment or infrastructure in which assets are located

The hacking and malware threat action varieties occur most frequently (and very often together), with the social threat action variety occurring third (and which is typically a precursor to hacking and malware):

HE-1: Financial Pretexting – the Golden Fleece

🛡 Breach scenario

Breach scenario
Specific

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Confidentiality, Integrity

🕐 Incident pattern

Pattern
Everything else

Time to discovery
H — D — W — M — Y

Time to containment
H — D — W — M — Y

⚠ Threat actor

Composition
Organized crime

Motives
Financial

Tactics and techniques
Use of stolen credentials, Phishing, Pretexting

◎ Targeted victims

Industries
Financial, Information, Retail

Key stakeholders
Legal Counsel, Incident Commander

Countermeasures
CSC-6, CSC-7, CSC-14, CSC-17, CSC-19

Description
Financial pretexting involves threat actors leveraging underlying human emotions, such as empathy, curiosity, trust and fear to achieve financial gain. These schemes involve social engineering tactics, such as phishing emails, phone call, or in-person meetings.

Down to the Wire

Stakeholder

Chief Information Officer

The situation

I asked, "In this day and age, how is it even possible for threat actors to initiate fraudulent wire transfers?" Our Verizon RISK Team investigative response liaison replied, "It happens all the time. Threat actors use social engineering tactics to fool someone into processing a fraudulent wire transfer." I thought, sure, it happens all the time, but this couldn't possibly happen to us. After all, as the CIO, I provide written approval for all wire transfer transactions within our organization. I was confident we had enough checks and balances in place to avoid fraud occurring. Well, I'd soon learn the hard way that confidence doesn't always align with reality.

Just a few weeks after we'd had this conversation, I received a sharp knock on the door from our Finance Director. She had a manila folder in hand, a sure sign that an undesirable conversation was about to ensue, but nonetheless, I invited her in. She proceeded to tell me that as part of a monthly audit, the Finance Department was missing an international tax form for a wire transfer that had occurred three weeks prior. This missing form had prompted her to request it from the accountant who originally submitted the request for the wire transfer. When she asked him for the form, he could not recall the details of the transfer. Since I had "approved" the transfer, she thought she would ask me if I could offer some assistance in "jogging his memory."

> I provide written approval for all wire transfer transactions within our organization. I was confident we had enough checks and balances in place to avoid fraud occurring.

As part of our wire transfer process, our accounting team must first email an invoice to me (typically from a vendor) containing the company name, services provided, bank account information, and invoice amount. I review the invoice and reply by email with an "approve" or "deny." If approved, the accountant then forwards the email, invoice and tax form (if applicable) to our Wire Transfers Department. This department then reviews the information for accuracy and processes the wire transfer.

> I review the invoice and reply by email with an "approve" or "deny." If approved, the accountant then forwards the email, invoice and tax form to our Wire Transfers Department.

In this case, with the exception of the accompanying tax form (which isn't required immediately upon completing the wire transfer) ALL of these things happened; however, I too could not recall providing the approval for this wire transfer. To make matters worse, she dropped another bombshell on me when she showed me the email in which I had provided approval for another wire transfer to the same bank account just three days prior to the one in question. We weren't talking chump change here: This was a significant amount of money, like buying a Rolls-Royce Phantom in a couple of different colors kind of money. We knew then we had a problem on our hands and engaged the RISK Team to investigate.

Response and investigation

The RISK Team started by reviewing the email associated with the wire transfer. They examined the email header information, and confirmed the wire transfer request did in fact come from the accountant's internal corporate email address. However, they noticed something odd with my email address. It looked very similar and did contain my full name, but the email domain name was different from our corporate email by just one character!

> Numerous external IP addresses had been successfully logging into the accountant's email using email web access.

They also told us it was originating from an external email service. The RISK Team did some research and were able to confirm someone had registered a domain very similar to ours just a few days before the wire transfer emails were sent. We now knew how the threat actor was able to provide the approval email, but I still wanted to know how the emails originated from the accountant's corporate email account.

In looking to answer this question, the RISK Team continued their investigation by collecting evidence sources including the accountant's email archive, a memory dump from the accountant's laptop, and a forensic image of the laptop hard drive. The RISK Team also asked us to provide them with email web access logs, since our employees have the ability to access their email accounts from the internet.

After processing and analyzing the evidence they had gathered, the RISK Team reported that numerous external IP addresses had been successfully logging into the accountant's email using email web access. These logins started about a week prior to the wire transfer requests. By analyzing activity on the accountant's laptop at the time of the web email logins, the RISK Team was able to determine the accountant had received a phishing email from someone claiming to have paid a "late invoice." The email instructed the accountant to click a link and provide their "email domain credentials" to authenticate and review the payment receipt. Apparently, the accountant provided his email account credentials and then forgot to follow up on the fact that he didn't receive the payment receipt.

The threat actor used the accountant's credentials to log into his email account and study our wire transfer approval process by searching through emails. The threat actor even used previously sent invoices and tax forms to create the fake versions that were used for the fraudulent wire transfers. Using the knowledge he had gained, the threat actor fabricated an approval email chain that they sent to our Wire Transfers Department.

> The IT Security Team informed me that our tools weren't able to block the URL, because the accountant wasn't using the corporate network.

I have to admit, while the RISK Team was telling me all of this, I couldn't help but think about the amount of money that we had spent on IT security tools that should have prevented this. Specifically, when the RISK Team informed us that the uniform resource locator (URL) link contained in the email was "known to be malicious," I really started to wonder why our tools didn't block access to the URL. I immediately put our IT Security Team to work on getting an answer to this question. What they found was interesting.

It turns out our internal URL filtering tool did in fact block access to that URL from other systems within our network. So why didn't it block the accountant's access? Well, based on the RISK Team's forensic analysis, it was confirmed that the accountant had actually been connected to his personal Wi-Fi network. He was working from home the day the phishing email was received. The IT Security Team informed me that our tools weren't able to block the URL, because the accountant wasn't using the corporate network.

To this day, we are still working with law enforcement to figure out what happened to our money.

Lessons learned

So, to summarize the lessons learned from this engagement, below are the mitigation measures and the response measures:

Mitigation

- Require two-factor authentication for access to email from the internet.

- Prepend a marker (e.g., "Subject: [External] … ") to the subject line denoting externally originated emails.

- Require secondary authorization for wire transactions over a certain dollar amount.

- Require Virtual Private Network (VPN) access for telecommuters accessing the corporate environment.

- Provide, at least annually, user security awareness training.

Response

- Maintain sufficient logging of access to email accounts from external sources.

- Collect volatile data, memory dumps, and forensic disk images prior to system shutdown.

- Encourage and recognize employees who report potential security issues.

- Engage bank fraud investigators for assistance, when applicable.

- Engage law enforcement for assistance, when applicable.

Remote tech support scams

In November 2016, the Verizon Cyber Intelligence Center (VCIC) examined the RISK Team caseload for remote tech support scam incidents. The VCIC findings, excerpted below, included three patterns of remote tech support scams.[6]

In today's organizations, users expect IT helpdesk support via remote administration. In this environment, a tech support scammer's goal is to establish a remote session whereby malicious software is installed, data exfiltrated, or configuration changes are made. Several recent cases involving remote tech support scams are highlighted here, including tactics, tools, and procedures used by the threat actors to gain a remote session.

Case 1

1 – User encounters pop-up on corporate laptop with a suspicious activity warning	2 – User calls support number listed on the pop-up	3 – Scammer convinces user to visit "hxxp://anydesk.com and download/execute anydesk.exe"	4 – Scammer establishes session with corporate laptop

Case 2

1 – User receives unsolicited phone call after browsing non-business-related websites on corporate system	2 – Scammer directs user to visit "hxxp://client.teamviewer.com and download/execute teamviewer.exe"	3 – Scammer establishes session with corporate system

Case 3

1 – User receives unsolicited phone call regarding a qualifying refund	2 – Scammer convinces user to allow access to system via LogMeIn Rescue software	3 – User directed to scammer-controlled site that is actually a fake portal for a refund service	4 – Scammer establishes session and sniffs user's banking credentials

Even as threat actors evolve their tactics in carrying out remote tech support scams, there are general security practices that organizations can follow to lessen the chances of falling victim. The VCIC recommends considering the following:

- Restrict software installation rights to privileged users.

- Block access to popular remote access software sites.

- Establish policies and practices whereby users can verify the validity of any contact with personnel offering tech support.

- Maintain a whitelist of approved software and enforce at endpoints.

- Educate users that tech support would never instruct them to install additional software downloaded from the internet.

HE-2: Hacktivist Attack – the Epluribus Enum

🛡 Breach scenario

Breach scenario
Specific

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Confidentiality, Integrity

⌚ Incident pattern

Pattern
Web application attacks, DoS attacks

Time to discovery
H — **D** — W — M — Y

Time to containment
H — **D** — **W** — M — Y

⚠ Threat actor

Composition
Activist

Motives
Ideology, Grudge

Tactics and techniques
DoS, Unknown hacking, Backdoor, Use of backdoor or C2, C2

◎ Targeted victims

Industries
Financial, Public, Information

Key stakeholders
Legal Counsel, Corporate Communications, Incident Commander

Countermeasures
CSC-4, CSC-5, CSC-7, CSC-16, CSC-18

Description

Hacktivist attacks leverage hacking techniques as a form of activism; these differ from the multitude of other attack types by the unique motivation of the threat actor. Commonly a hacktivist is motivated by a desire to harm or embarrass their targeted victim in an effort to further a political or social agenda.

An Executive Doxxing Match

Stakeholder

Lead Investigator

The situation

The Verizon RISK Team was contacted by a multinational organization that had attracted negative attention following the handling of an unpopular company restructuring. This customer, Cheese Movers International (CMI), had a significant number of disgruntled employees and ex-employees. They had also drawn the attention of more than one group of hacktivists who had posted messages on their social media accounts referencing the changes. Various derogatory hashtags on social media were popping up and threats against executives were being posted to social networking sites.

The customer was a soft target for hacktivism; their attack surface was large due to their sheer size and their diverse, global business units. This was exacerbated further by the risk of an insider threat or recently terminated ex-employee using their advanced knowledge of the organization to perpetrate an attack or to leak information assisting other threat actors.

On the face of it, there was no evidence that any attack had been initiated; however, CMI sought our assistance to help them proactively gather threat intelligence, perform penetration testing, and be prepared should any of the online threats materialize.

Response and investigation

We initially provided CMI with assistance and guidance in collating and reviewing open-source intelligence; this included searching social networks and online forums as well as specialized investigative activities within the darknet, the less accessible part of the internet, which is anonymized by protective software and configurations. We set up a secure anonymous account of our own, which enabled us to search through marketplaces and other locations on the darknet to see what the hacktivists were discussing in relation to CMI. These activities identified a huge number of threats and negative statements. And although the majority was not considered genuine, the home address and personal details of executives were being actively sought by suspicious parties.

> The customer was a soft target for hacktivism; their attack surface was large due to their sheer size and their diverse, global business units.

Later on, evidence was found that personal details for two executives had been obtained and were being shared online. CMI was able to implement the Incident Response (IR) Plan they had developed to deal with this type of situation as it arose. The breach of personal information associated with senior executives was identified early enough that it could be reported to Law Enforcement (LE) before malicious parties acted upon it; as a result, the ensuing threatening phone calls and spurious deliveries were monitored from the outset and were immediately followed up. Local LE also provided a liaison officer and guidance on physical protection considering the threats that had been received.

Unfortunately, this was just the first of multiple threats and attacks experienced over the course of the next three weeks. Distributed Denial of Service (DDoS) attacks were attempted against many of the company's websites. The majority of these were thwarted by the DDoS protection capability that CMI had put in place as a result of the intelligence provided by our Verizon Cyber Intelligence Center (VCIC) and our Darknet Research Team.

We collaborated with our Pen Testing Team to perform urgent assessments of key assets. Due to the very short timeframe, these assessments were performed on a best effort basis, but they successfully identified vulnerabilities in web-facing servers which could have proven catastrophic had they been noticed by hacktivists. In two cases, a Structured Query Language (SQL) injection vulnerability and an unpatched application with known vulnerabilities were identified. It was later found that both servers had been targeted with reconnaissance activities, which may have identified the same vulnerabilities had they not been urgently patched by CMI.

After approximately two weeks of successfully defending against attacks on all fronts, an attack was finally successful. One of CMI's websites appeared to have been defaced: The site was not accessible and had been replaced with a message claiming responsibility and blaming CMI for inviting this retribution. The posted message claimed that CMI servers had been hacked and customer data would be leaked unless certain actions were performed. We quickly determined the defacement did not appear to be the result of a compromised CMI system, but rather visitors to the relevant Uniform Resource Locator (URL) were being redirected to another server hosting the message.

As a matter of due diligence, we deployed our investigators to the datacenter containing the affected web server. We quickly confirmed that no evidence of a breach existed. Furthermore, our RISK Network Forensics (NetFor) Team, who had previously deployed full packet capture devices within four data centers, had not identified any suspicious or malicious traffic.

It was later determined that the domain registrar for the effected domain had been targeted in a social engineering attack, during which the threat actor successfully impersonated CMI staff. They were able to gain access to the account on the domain registrar's service and modify the relevant Domain Name System (DNS) records, which caused visitors to the CMI URL to be redirected to another website.

Fortunately, the site in question was not CMI's principal website and was only used by a small subset of their customers. The DNS issue was quickly resolved and eventually this domain was migrated to their principal domain registrar, whose security practices were superior.

As with many similar incidents the media attention soon dried up as did the interest of the hacktivists. The DDoS attacks became less and less frequent and the internet was soon engulfed in the next drama. CMI maintained extra vigilance for a number of months, but before long, it was back to business as usual.

Lessons learned

The information gathered from intelligence sources was vital in our response efforts, as it provided us with the knowledge of who the targeted victims were, and the tactics the threat actors would deploy. Mitigation and response activities are as follows:

Mitigation

- **Don't rock the boat.** Stay off the radar of any potential hacker.

- **Keep an ear to the ground.** Base defenses, detection mechanisms and response capabilities on sound threat intelligence.

- **Secure your environment.** Implement a timely and effective patch management program; conduct regular penetration-testing activities.

- **Protect social media accounts.** Use two-factor authentication, strong and varied passwords, as well as proper security awareness training for staffs who manage the social media presence.

- **Protect third-party services.** Protect account credentials; use a reputable domain name registrar that offers two-factor authentication or approved IP address whitelisting[7].

Response

- **Prepare and initiate your IR Plan.** Establish an IR Plan early, and then regularly review, test and update it.

- **Scope and triage the incident quickly.** Effectively scope and task prioritize; be prepared to manage simultaneous, yet distinct, incidents.

- **Proactively communicate with affected entities.** Confirm facts quickly; develop a remediation strategy and communicate this to customers.

- **Engage LE at the right time.** Consider legal and regulatory responsibilities in conjunction with advice from Legal Counsel; contact LE when the time is right.

---

7. For further details on the recommendations above, see "Data Breach Digest – October 2016 Update, Hacktivist Attack: Shedding Light on the Matter" at www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2016/.

What's in a name? The Domain Name System

The Domain Name System (DNS) enables people and machines to communicate across the internet without memorizing lengthy IP addresses. Similar to a phonebook, the DNS protocol translates human-friendly domain names such as "Verizon.com" into machine-friendly IP addresses such as IP 192.16.31.23, and vice-versa. This lookup is critical to modern networks and touches almost every host connected in some manner. Threat actors have found that DNS can be misused in a variety of ways, including using its pervasiveness against otherwise hardened networks.

One drawback of the distributed nature of DNS is that it allows threat actors to use the name system to reflect or amplify Denial of Service attacks. By requesting domains from a large number of public DNS servers, often with spoofed source IP addresses, additional load can be placed on the target, eventually crippling their ability to respond to requests. While web servers and other infrastructure may still be running without issue, the general inability to resolve domain to IP address will prevent the majority of users from accessing websites or other applications.

Threat actors can also leverage DNS to covertly exfiltrate data, even in networks with good security controls in place. DNS traffic to and from external hosts is common and frequently escapes the scrutiny of security teams. The large volume of this type of traffic makes reviewing each request impossible and DNS logs are often forgone for other solutions, such as intrusion detection systems (IDS), which may not identify this type of exfiltration. This leaves threat actors with the ability to embed data into DNS requests and bypass security controls, which would otherwise prevent outbound traffic from protected hosts.

As with exfiltration, DNS's wide reach allows threat actors to maintain persistence into compromised networks via techniques such as FastFlux DNS. In cases like this, malware on infected machines contain Domain Generation Algorithms (DGAs) which programmatically produce thousands of potentially malicious domains. The malware then checks each domain, looking for an IP address or other response from a remote DNS server. Through this method, new command and control points can be defined, allowing threat actors to evade reputation-based blacklisting.

Attack-Defend Card

HE-3: Partner Misuse – the Indignant Mole

Breach scenario

Breach scenario
Specific

Sophistication level
1 2 3 4 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Insider and privilege misuse

Time to discovery
H D W M Y

Time to containment
H D W M Y

Threat actor

Composition
Other (Partner)

Motives
Financial, Espionage, Grudge

Tactics and techniques
Data mishandling, Net misuse, Privilege abuse

Targeted victim

Industries
Accommodation, Financial, Retail, Healthcare

Key stakeholders
Legal Counsel, Incident Commander, Corporate Communications

Countermeasures
CSC-6, CSC-12, CSC-13, CSC-16, CSC-19

Description

Partner misuse involves semi-trusted entities who have some level of enterprise environment access and, either through purposeful maliciousness or inadvertent ineptitude, lead to a breach of that environment.

The Broken Circle of Trust

Stakeholder

Legal Counsel

The Situation

As a partner in a global law firm, I have 25 years of experience assisting clients who manage various litigation and employment issues resulting from data breaches. Without necessarily realizing it, I've been working in the "data breach" industry for many years, be it advising my clients on internal investigations and associated litigation involving cybersecurity and privacy issues, or helping them meet their regulatory requirements following inadvertent data disclosures.

> [The company was] seeking my advice regarding their obligations concerning data protection and other relevant cybersecurity legislation.

Recently one of our clients, a regional water supplier, contacted my firm to discuss an incident that affected several of their small and medium-sized enterprise clients. Their clients had recently notified them that their online account details had changed. The company had wisely identified the potential that customer data had been compromised and they were seeking my advice regarding their obligations concerning data protection and other relevant cybersecurity legislation.

Unfortunately, as our conversation progressed, the issue extended beyond a simple data breach. When customers had their passwords reset and regained access to their accounts, many noticed that the registered bank account details had also been changed. This meant that refunds due to the customers had been transferred fraudulently to new bank accounts. It was later determined that the refunds totaled over £500,000 and were directed to two bank accounts in England.

I subsequently worked with Law Enforcement (LE) and the National Action Fraud Hotline to track down the bank account holder. As I did so, it became clear that the banks had also been socially engineered. Believing the refunds to be foreign deposits, they allowed the account holder to transfer 90% of the money to accounts in Dubai and the Bahamas as soon as the payments arrived in their UK account. Ultimately, the funds had been withdrawn from the accounts and used to purchase Bitcoin, which was transferred to addresses associated with a Bitcoin mixing (laundering) service. The trail went cold and the LE inquiries failed to identify a subject.

After several discussions with my client, it was obvious they had had a data breach. What wasn't obvious was how the breach occurred. Despite a robust security posture, none of their security appliances or log sources showed any signs of compromise. A review of affected accounts and systems showed no signs of malware or tampering. With my client's approval, I reached out to the Verizon RISK Team for assistance in the investigation – hoping desperately that they could turn up some new evidence.

Threat targeting: Attention small business owners!

Small business owners often consider themselves as an unlikely target, believing themselves to be a smaller fish in the sea for an attacker. However, this feeling evidently provides a false sense of security when we consider the high amount of secondary attacks conducted from compromised systems.

Attackers often compromise smaller less secure businesses and use their environments as their base of operations. The attackers rely on relatively insecure systems with poor monitoring and logging as an additional layer of security when perpetrating attacks. Your systems might be the origin of major breaches and, in addition, your intellectual property might be an attractive bonus.

Response and investigation

Once the RISK Team arrived at my client's premises, a "war room" was established and the discussions turned to network diagrams, web servers, log files and payment and refund flows. While some of the technical details went over my head, the RISK Team hit the proverbial ground running. They were quickly able to establish all the systems and processes involved in managing the customer account creation and storage.

> A "war room" was established and the discussions turned to network diagrams, web servers, log files and payment and refund flows.

The RISK Team did a due diligence review of various logs and the web server itself. Using their listing of known Indicators of Compromise (IoCs) they confirmed that no malicious software was present. With very little to go on from a technical standpoint, the RISK Team lead investigator suggested we speak with some of the people involved. I expressed my concerns – it would be a large project to interview so many people, and many employees were remotely located in India. The RISK Team investigator assured me this was nothing new for his team and he already had resources lined up in India ready to travel onsite.

Agreeing to the plan, my customer allowed the RISK Team to conduct interviews with various stakeholders including those identified at a third-party call center in Mumbai, India. This call center was responsible for administering the online accounts and processing telephone payments. Two RISK Team investigators arrived in Mumbai to interview the third-party call center personnel. During the interview, and subsequent review of the Customer Relationship Management (CRM) log files, it became evident that one user had accessed all the accounts that had been fraudulently refunded.

An investigation of the user's computer confirmed the access to my client's Content Management System (CMS) records in question; however, there was nothing to suggest the data had been copied or that the refunds had been requested using this computer. The user denied any knowledge of the fraudulent activity and suggested the computer must have been hacked, although the RISK Team's analysis identified no such evidence. The user was so adamant that he was not involved that to "prove" it he signed an affidavit that permitted the RISK Team to examine his home computer.

Security imperative: Multi-factor authentication

Multi-Factor Authentication (MFA) is an access control system that allows users to authenticate to resources using two or more independent forms of identification. These fall into the categories of something you know, such as a user-created password, something you have, such as a one-time passcode (OTP), and someone you are, such as your fingerprint or retina scan. A unique OTP is typically generated every 60-90 seconds on a physical dongle or within an application. This requires physical possession to be read (thereby aligning with the "something you have" factor). Many users may have an application installed on their smartphone through which they can obtain the OTP at any time.

When a user authenticates to an MFA system, the system first checks that it has received the correct user-created password (something you know). Next it checks the OTP (something you have), which is known only to the user and the MFA system. Only when these two pieces of information are correct does the MFA system allow the user to authenticate successfully.

An alternative method of MFA involves a known password and a biometric scan for authentication. Using this method, a user may authenticate by providing a user-created password (something you know) in addition to a biometric scan (something you are). These biometric scans are typically done on a user's fingerprint or retina, as these are unique to each individual. Additionally, many hardware and software developers have started to introduce facial recognition technology as a means of biometric authentication.

An initial review of the user's home computer system revealed very little data. In fact, so little was found on the system that it appeared to have been systematically cleaned using data wiping software. Unfortunately, for the user, the wiping software did not fully clean the volume. Shadow copies of data were recovered revealing numerous email messages between the call center employee and another individual, later identified to be his cousin in the UK. These emails contained pictures of account details that correlated to the accounts affected by the fraudulent activity. The RISK Team pointed out that the metadata within these photos indicated that they had been taken with a camera phone and the photos appeared to be of a computer system monitor.

> Shadow copies of data were recovered revealing numerous email messages between the call center employee and another individual, later identified to be his cousin in the UK.

With new evidence in hand, the RISK Team returned to the Mumbai office for a follow-up interview with the suspected worker. When presented with the data retrieved from his home computer, the worker finally confessed to the crime and offered assistance in identifying accounts with over £1,000 in refunds stolen.

Working with LE and the RISK Team, a plan was hatched to verify the identity of the employee's cousin. The employee would take a photograph of the account details and would send the picture to his cousin in England, who would then create an online account or request a password reset for their current account as he had in the past. Once we validated the change was in place, we took the phone number and log file evidence to the authorities to secure a conviction.

Lessons learned

It's always good to sit back, relax, and reflect after an incident. The main points of consideration coming out of this incident would be to review in-place agreements with partners who have access to your critical data and that they conduct stringent background checks on their employees. Typical mitigation and response actions to take for partner misuse situations are:

Mitigation

- Monitor corporate and guest network activity.

- Take steps to reduce external device threats.

- Keep tabs on sensitive data.

- Be cognizant of changes in employee attitude/behavior.

- Establish a Data Classification Policy (and limit printing copies).

Response

- Prepare and initiate your IR Plan in a timely manner.

- Quickly scope and triage the incident.

- Proactively communicate with affected entities.

- Seek advice from Legal Counsel; contact LE when the time is right.

Partner threat: the Goldilocks zone

As science continues to search for intelligent life in the cosmos, new strategies are employed to separate the metaphorical wheat from the chaff. One such example is to concentrate on planets located in the 'Goldilocks zone'. In other words, they search for planets that are not too hot, not too cold, not too big, and not too small, but just right to increase the likelihood of supporting life, and perhaps intelligent life.

That concept, in an adapted form, also works well for us old-fashioned earthbound folks when it comes to doing business with partners. You need them close enough to rely on, to interact as seamlessly as possible, to allow for free-flowing communication and data, but not so close that you catch whatever they may have. Over the years, our corpus has continued to show that partners are not as great a threat as might be commonly thought. Partner threats fall into three main categories:

- **Credentials**. Criminals leveraging partner credentials to get into your network (e.g., the bad guys obtain the username and password that your partners utilize to access your systems).

- **Maliciousness**. The partner misuses their access to your systems to download, modify, or otherwise do bad things with your data. This is similar to an insider threat, only with modified privilege levels.

- **Error.** The partner made a simple error that affected you negatively. A common example of this is utilizing a third-party to manage a website or outsource your billing. The partner sends the wrong information to the incorrect recipient or makes something publicly viewable by mistake.

The main lesson here is to do what you can to make sure that the partners you choose are reputable and have a robust security program of their own. You should also limit the access and privileges your partners have on your systems to reduce the impact of any nefarious activity, and for that matter, any inadvertent damaging errors.

HE-4: Disgruntled Employee – the Absolute Zero

Breach scenario

Breach scenario
Specific

Sophistication level
1 — **2** — 3 — 4 — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Insider and privilege misuse

Time to discovery
H — **D** — W — M — Y

Time to containment
H — **D** — **W** — M — Y

Threat actor

Composition
Other (Employee)

Motives
Grudge, Espionage

Tactics and techniques
Export data, Privilege abuse, Capture stored data, Disable controls

Targeted victim

Industries
Public, Financial, Healthcare

Key stakeholders
Human Resources, Legal Counsel, Incident Commander

Countermeasures
CSC-1, CSC-6, CSC-10, CSC-13, CSC-16

Description

Disgruntled employees, especially those disillusioned with their company, can represent one of the most difficult threat actors against which to defend. Layoffs, pay cuts, or organizational shifts may leave some employees in a position where they can rationalize nefarious activities.

A "Pre-Competitive" Advantage

The Situation

By definition, employees have access to privileged systems and information; this means large amounts of legitimate activity will need to be sorted through during breach response efforts. Any employee can be angry enough to do something malicious, and therefore special care needs to be taken around events that can increase employee emotions.

Firing people was rarely an interesting job, but as I sat filling out the final forms for terminating Mr. Simpson, I breathed a sigh of relief, glad to be done with the ordeal. On the surface, it seemed like a straightforward case. Mr. Simpson's team was being merged with another team and he was unhappy with the new hierarchy. After being informed by a friend in Human Resources (HR) about the upcoming changes, Mr. Simpson began using his administrative access to take over other accounts. He ultimately attempted to disrupt operations — a vindictive response to being underappreciated — and downloaded confidential files (a bargaining chip for this next job). It seemed so cut and dried — he did it and admitted to it — but still the lawyers required us to collect the evidence to prove it.

Response and investigation

I don't imagine most investigations begin with the answer, but with a very candid confession from the primary suspect, ours did. We knew how, when, and what happened from Mr. Simpson's description and by the time we engaged the Verizon RISK Team, all we needed them to do was document and verify the claims from a technical point of view. Once we knew we had the whole truth, I could then expect to fill out a stack of forms to safely terminate Mr. Simpson's employment.

The events that led to Mr. Simpson's confession were well-documented. On an otherwise normal Friday afternoon, a programmer reported that an application was experiencing unexpected failures and an internal investigation began. This investigation turned up multiple suspicious log entries showing Mr. Simpson logging into the application server only minutes before the problems started. The logs showed failed super user account access from Mr. Simpson, followed by password resets of service accounts. These findings could potentially have been legitimate as Mr. Simpson was an IT administrator, but the circumstances surrounding them — no ticket or prior notification — led to the interviews in which he eventually revealed his actions, in hopes of leniency.

Incident pattern: Insider and privilege misuse

The "Privilege Misuse" pattern is one of the few that includes collusion between internal and external actors. According to VERIS, the top industries affected by this are the public sector, healthcare, and finance organizations. This category covers the insider threat, but can also include external actors collaborating with internal actors to gain unapproved or malicious use of organizational resources.

Financial gain and espionage remain the primary motivation for committing this type of attack. The most common form of misuse is merely using access to gain information for alternative and unsanctioned uses. The weakest link for any organization is not its systems, but rather the human factor. It is important to note that these incidents are not always the result of a malicious employee and often stem from carelessness and lack of awareness regarding sound IT protocol.

Insider threats are usually the most difficult to detect and can take months, or longer, to discover. Identifying insider privilege abuse can be difficult because it is often committed by employees perceived to be trustworthy, and because they are using the privileges granted to them by the organization. Organizations should proactively take steps to minimize the privileges users are provided with. They should also keep detailed audit logs of users with administrative privileges.

In addition to the known application server activities, Mr. Simpson admitted to accessing multiple email boxes using the service accounts to collect data for interview use and to insert scheduled jobs designed to disrupt his new team's workflows. This was a lot of data to sort through, and I honestly didn't know where to begin looking to verify these claims. Thankfully, our IT Security Department had called in the RISK Team to assist in the digital forensic examination to determine if Mr. Simpson had left any other surprises for us to find.

The RISK Team requested a huge number of log files and mailbox summaries, and immediately started digging in. It was only the next day when preliminary findings began coming back to us. The investigators verified that Mr. Simpson had used his access to compromise other accounts. Much to my surprise, included in their initial findings was a listing of every file he had downloaded from another user's inbox, which looked like it included everything from operations documents to product technical details. This was more than a bargaining chip. This was corporate theft. Beyond the stolen files was a second listing of scheduled jobs inserted by Mr. Simpson. The jobs were exclusively mass delete commands scheduled to occur at critical times over the next year: During tax season, prior to holiday bonuses, and a few seemingly random dates.

> The jobs were exclusively mass delete commands scheduled to occur at critical times over the next year: During tax season, prior to holiday bonuses, and a few seemingly random dates.

While our internal teams worked to remove the jobs and validate the contents of each stolen file, the RISK Team investigators moved on to their second phase - discovering any other activity to which Mr. Simpson may not have confessed. After requesting "network logs" from our IT Security Team, the investigators turned to searching for known threat actors and suspicious activity. They also focused analysis on the time range defined by the service account compromises. A few days and a dozen email requests later, a second set of findings arrived from the RISK Team.

The RISK Team review of the network traffic had identified suspicious connections to a server in Romania. This particular server was owned by a short-term lease hosting location using Bitcoin as payment. The report explained that this was currency used frequently by hackers wishing to remain anonymous, and while completely unrelated to Mr. Simpson's activity, many other attacks had involved this system. Closing out the findings was a set of instructions for our IT Security Team on how to find and identify the internal system in question.

> [Bitcoin] was currency used frequently by hackers wishing to remain anonymous, and while completely unrelated to Mr. Simpson's activity, many other attacks had involved this system.

It took our IT Security Team only a few hours to find the suspicious system and remove it from the network for further review. The onsite RISK Team investigators collected a forensic system image and shipped it to the RISK Labs for examination. This proved fruitless; comparisons with known malicious files and analysis of changes around the time of the network activity revealed nothing. Both the IT Security Team and RISK Team were baffled, as the traffic was definitely coming from this system and had stopped immediately after the device was taken offline; however, nothing seemed to be out of place. We were getting antsy.

Returning to the physical device, the RISK Team investigators began to collect additional forensic information and had a lucky break. While plugging in a USB keyboard to issue commands, the investigator noticed an extension on the plug itself. When pried, it popped off, revealing an off-the-shelf, clandestine keylogger. The RISK Team explained that the keylogger was designed to capture any input a user provided via the keyboard and was sending the capture to the rented Romanian server. I was stunned; this was the kind of thing I thought I'd see in a movie, not my job, but the proof was there in our hands.

Mr. Simpson's actions were vindictive and done in response to the recent restructuring of the company's IT Department. One of Mr. Simpson's main motivations was to make the new IT Department appear incompetent. He had admitted that he was planning to use the information he stole as leverage in finding a job with a competitor and possibly profit from his exploits. Finally, he had lied about the extent of his actions and clearly had gone beyond simply being upset. With the evidence and paperwork in hand, Mr. Simpson was summarily fired and the forensic reports were provided to law enforcement.

> While plugging in a USB keyboard to issue commands, the investigator noticed an extension on the plug itself. When pried, it popped off, revealing an off-the-shelf, clandestine keylogger.

Lessons learned

Our company narrowly dodged a bullet in that some of our most sensitive information and intellectual property was nearly stolen; we learned several lessons as a result of this incident. One lesson was that the friend in HR should not have notified Mr. Simpson. Details regarding restructuring and moving of specific jobs should be closely held and carefully coordinated with department managers. Another was the company should have had an action plan in place, such as increased monitoring of employees affected by the transition, to reduce the risk of vindictive behavior by those affected. Finally, as part of the transition, the company should also have conducted a thorough asset inventory. Doing so might have identified any installed keyloggers.

Actionable intelligence: No, it's not an oxymoron

Some say the two words "actionable intelligence" together form an oxymoron. However, in cybersecurity parlance it has a very critical objective by the virtue of being (a) actionable; i.e., a clear set of actions or countermeasures that can help prevent or detect a cyberattack and (b) intelligence; i.e., sometimes abstract but relevant knowledge that can help pinpoint a cybersecurity event, trend, pattern or incident from the perspective of known-unknowns as well as unknown-unknowns.

Actionable intelligence is derived from telltale signs or early threat warnings based on external information or feeds, and internal threat hunting efforts. This should ideally be specific enough to identify compromised assets, usable as an indicator of compromise and, most importantly, consumable by prevention and detection security platforms. There has to be a clear difference between "raw information" or "information overload" and the real "actionable intelligence." Organizations should try to elevate their focus from having access to indicators of compromise to indicators of anomalies.

Threat actors: Insider threat motivations, misdeeds and miscues ...

Common motivators for insider threats consist of financial gains, revenge, excitement, patriotism, and ideological motives. These motivators could stem from greed, vulnerability to blackmail, feelings of entitlement, or lack of loyalty.

Detecting insider threats can be difficult as it may involve identifying personality characteristics of individuals based on these motivators. Being vigilant can help identify an insider threat before an attack is conducted. In terms of potentially suspicious activities, these may include accessing company resources after business hours, an undue interest in information outside of their job function, and accessing resources beyond their common workspace.

Fortunately, multiple solutions exist for detecting malicious behavior within the environment. In terms of technology solutions, Data Loss Prevention (DLP) and Security Information and Event Management (SIEM) solutions can detect unauthorized access and unusual data flow. In addition to a technological approach, supervisors and employees should be sensitized to detect and report suspicious behavior or situations, which may lead to insider threats.

Deterrence comes in many forms, but most focus on creating a positive at-work experience for employees. Employees should have methods of voicing dissatisfaction toward the workplace. This may prevent possible disgruntled employees from taking malicious action before they begin by giving them an approved outlet for their frustrations. Recognition of positive performance is also important as it may help nurture loyalty or satisfy ego-driven employees. No situation is completely avoidable and there will always be a vengeful ex-employee to consider. However, open dialog and ample documentation of employee interactions during the transition phase will help ensure both the employer and employee are represented fairly.

Spotting email phishing in 1-2-3 steps ...

Upon receiving an unsolicited or suspicious email, a 1-2-3 step approach to assessing whether or not the email is malicious consists of scrutinizing the email message, any embedded hyperlinks, and any attached files.

1 – Email message
The first component of an unsolicited email to review is the email message itself. Indicators that an email may have been spoofed or sent by a suspicious threat actor can be seen below:

Look carefully at the sender's email address. Look for typos or mismatched email domain names.

Be cautious of messages that require urgent and immediate action.

Embedded links should always be approached with caution. Hover your mouse over the link to reveal the domain name.

Balance Overdue!
Kimberly Jones <kjones@spoofedemailaddress.com>
Sent: Mon 10/17/16 5:09 PM
To: Smith, John
Cc:

Dear Mr. Smith,

Payment for invoice #4327394 is over 90 days late. Please click here to pay now and avoid being sent to collections.

Regards,
The Roman Holiday
Account Representative

2 – Email hyperlink
The second component of an unsolicited email to review is any hyperlinks contained in the message. Indicators of malicious links contained within an email will often take the following forms:
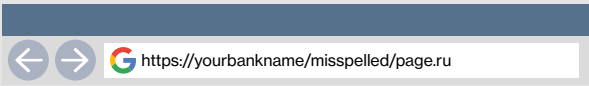
Look out for spoofed links to seemingly legitimate sites.

Hover your mouse over the link to see the actual destination.

Dear Customer,

The password for your bank account has expired. Please go to www.yourbankname.com now to change your password.

Sincerely,

https://yourbankname/misspelled/page.ru

Check the URL to ensure the domain name matches. Links in phishing emails will usually redirect you to a spoofed website. Watch carefully for misspelled names (e.g. www.gatorgrazpfasteners.com).

Check the country code in the domain in the URL. Be suspicious of country codes that do not match up with the organization.

3 – Email attachment
The third component of an unsolicited email to review is any files attached to the message attachments. Indicators of undesirable attachments to incoming messages may be:

Security warnings could indicate embedded malware. Opening these files may launch or install malware.

Security warning

Protected view

Beware of compressed and/or encrypted attachments. —— Invoice.zip

Taking this three-step approach to assessing whether or not an email is malicious will help in preventing or mitigating the effect of phishing campaigns.

Conduit Devices

As with humans, devices also play a substantial role in data breaches. Vulnerable devices can be targeted because of the data they store or process and are often used by threat actors as Command and Control (C2) platforms or pass-through intermediaries. Conduit devices consist of networking equipment, servers, desktops, laptops, tablets, smartphones and portable storage devices. This represents an unending list of devices to protect and monitor.

A more focused approach to mitigating conduit devices is to consider what makes a device desirable to threat actors: 1) the data it stores or processes, 2) known device vulnerabilities, and 3) accessibility to the internet (e.g., desktops via SMTP, web browsers and web applications).

Scenario CD-1 (C2 Takeover) describes a server taken over by threat actors and used as a command and control platform. Scenario CD-2 (Mobile Assault) recounts a traveler and their laptop and smartphone being targeted by threat actors, while Scenario CD-3 (IoT Calamity) describes an overwhelming volume of DNS lookups associated with IoT devices. Scenario CD-4 (USB Infection) tells the story of an insider threat plugging in a USB storage device to multiple systems.

Top five asset varieties (conduit devices) within the VERIS data over the previous three years for data breaches:

Ranking	Asset	Frequency
1.	Desktop	37.6%
2.	Web application	32.9%
3.	Human beings	32.3%
4.	POS controller	22.1%
5.	POS terminal	20.4%

Incident pattern: Payment card skimmers

While this year we don't have a scenario particular to the "payment card skimmers" incident pattern, we thought we'd touch on it briefly here …

Payment card skimming is a tried-and-true attack method used by threat actors, from both organized crime groups and lone wolves seeking to try their hand at a known method with a high-degree of success. Frequently unattended card readers, such as ATMs and gas pumps, are targeted since the chance of discovery by unassuming customers is low. However, any device that reads payment card data from magnetic stripes is vulnerable and it should be treated as such by both users and IT Security personnel alike.

Skimming devices present a very low barrier to entry for fraudsters. Many are available for only a few hundred dollars from online marketplaces and are manufactured precisely to be inconspicuous on the targeted system. Once collected, threat actors are able to write the stolen data to a new card's magnetic stripe and use the fraudulent card to make transactions.

Available data suggests that detection and reporting of this attack method does not keep pace with its prevalence; alerts are triggered most often by fraud detection software on post-attack transactions. By that time, threat actors will likely already be on the move, taking their skimming device in search of new targets. Consequently, being able to spot the abnormal is critical in thwarting payment card skimming. Readily visible tamper indicators and regular inspection by the IT Security Team can go a long way to reducing the problem, as can the immediate reporting of suspected fraud by card users.

CD-1: C2 Takeover – the Broken Arrow

Breach scenario

Breach scenario
Specific (espionage), Opportunistic (financial)

Sophistication level
1 — 2 — **3** — **4** — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Web application attacks, POS intrusions, Cyber-espionage

Time to discovery
H — D — W — M — Y

Time to containment
H — D — W — M — Y

Threat actor

Composition
Organized crime, State-affiliated, Activist

Motives
Financial, Espionage, Grudge

Tactics and techniques
Use of backdoor, C2, Scan network, Rootkit

Targeted victims

Industries
Information, Financial, Public, Administrative, Manufacturing

Key stakeholders
Incident Commander, Legal Counsel

Countermeasures
CSC-3, CSC-11, CSC-12, CSC-16, CSC-19

Description
Command and Control (C2) takeover denotes compromised systems leveraged by threat actors for nefarious purposes. Prior to takeover, these legitimate systems were likely unpatched or unmonitored, and thus an attractive target for threat actors to leverage as their C2 infrastructure.

Platform of Destruction

Stakeholder

Network Forensics Specialist

The Situation

Threat actors invest large amounts of time into compromising environments for malicious purposes, and as such, the Verizon RISK Team frequently sees instances involving a single environment used for multiple purposes. This search by threat actors for maximum return on investment means that even if a known compromise is remediated, due diligence is essential to rule out other nefarious activities.

> This search by threat actors for maximum return on investment means that even if a known compromise is remediated, due diligence is essential to rule out other nefarious activities.

"Nothing can hide on the network," Sally thought to herself as she reviewed the day's listing of threat actor activity. Sally was part of a small team of analysts who, for the past couple of months, had been monitoring network traffic, and tracking C2 operations at a compromised location. Each day automated scripts churned through millions of individual packets searching for patterns that indicated beaconing traffic between remote systems and compromised endpoints.

It was Sally's job to review this output and determine if the systems identified were newly infected systems reaching back for instructions. Today's listing included multiple new entries – government entities, multinational corporations and even a university. Sally painstakingly recorded the findings in a report sent daily to law enforcement working to handle the threat on a larger scale.

Historically, only C2 activity had been identified at this location; however, as part of her daily routine, Sally conducted a proactive review of other traffic captured. She soon stumbled upon various outbound Simple Mail Transfer Protocol (SMTP) traffic destined to IP addresses associated with recently compromised entities.

Analyzing the traffic further, Sally discovered emails with links that resolved back to files on the C2 server that were sent only a few hours before the first infected system connected to the C2 server. These emails contained content related to current events and appeared to be precursors to organizations being affected. This looked to be part of a phishing campaign, a very common method used to compromise organizations. She added a few notes to her daily report and then sent it along.

Malware command and control

Our 2016 DBIR showed that while many capabilities exist within the types of malware we observe, almost all involve some form of C2 or backdoor access functionality. In the case of attacks on web applications, the vast majority of incidents involved an infected server receiving commands via these channels or being actively used as the command server itself.

The fact that most malware requires this network-based C2 infrastructure allows incident responders to identify infections, regardless of malware variant or capabilities, by investigating suspicious or unexpected network connections. In many cases, this is not as straightforward as it may seem, as production servers often have hundreds or thousands of remote connections. By leveraging lists of known indicators, heuristic tools designed to identify malware-like patterns (such as beaconing), or analyzing traffic to identify suspicious behaviors, investigators can target systems for deeper review.

Response and investigation

The next day Sally and her team met to discuss what changes they should make considering the new information. If the threat actors were expanding their operations at this location, new automation and additional review procedures would need to be created. While the developers began identifying ways to automate finding the initial emails, she turned back to the packet captures to see if anything else was hiding among the regular traffic.

Looking for new and suspicious activity in this data set was not trivial as the location being monitored was a legitimate hosting provider with dozens of non-malicious websites being accessed by end users. Sifting through all the expected traffic to find unknown malicious activity was a time-consuming process, but Sally enjoyed the challenge. Leveraging metadata collected from the packets, she pivoted between connections searching for abnormal behavior. After having spent time learning what was normal traffic or activity in the environment, communications, which were out of place jumped out at her. Sally continued slowly eliminating sets of data until she came across several unusual outbound connections.

> While the developers began identifying ways to automate finding the initial emails, she turned back to the packet captures to see if anything else was hiding among the regular traffic.

She had identified a single internal system, designated as a database server, making sporadic Hypertext Transfer Protocol (HTTP) requests to a diverse set of external domains. Outbound web traffic was not normal for this database server and the sessions themselves showed signs of being automated, rather than driven by a real user. Each request lacked headers typically associated with browser-based HTTP traffic, and the pages requested were limited to single pages with supporting style sheets; JavaScript and images were ignored completely. This type of activity screamed "automation" and Sally was very curious as to its purpose.

> In addition to moving the phishing and exploitation operations over to this environment, it seemed the threat actors were conducting initial reconnaissance on other potential targets.

Sally collected a list of all distinct remote domain names; it didn't take long before a few items jumped out at her. This list – or at least parts of it – consisted of targets that had been identified previously as compromised organizations. In addition to moving the phishing and exploitation operations over to this environment, it seemed the threat actors were conducting initial reconnaissance on other potential targets. This finding was critical because it meant Sally and her team could now track the entire threat actor's processes from recon to post-infection. She quickly captured the details and results of each query and provided them to the development team for automation. Once these new tasks were automated, the information collected could be included in the daily reports, which could be reviewed and shared with Law Enforcement (LE).

With the reports now including a listing of potential targets (based on the reconnaissance) and solicited targets (based on the SMTP traffic), Sally and other analysts could begin enumerating deeper levels of the threat actor's strategy. This process allowed Sally to gain insight into trends related to the threat actor's prioritization. Many searches appeared for lesser-known online retail providers; however, only a subset of the total searches was targeted for attack. The difference between these two lists allowed Sally to do a comparative analysis and determine what criteria the threat actor was using to select targets. Current targets appeared to be limited to customers running a version of the Apache webserver with a known remote code execution vulnerability. This was determined by reviewing the server-side responses showing the version of Apache in use across the targets.

The delta between targeted and affected organizations also provided insight into mitigation methods that might be successful or organizations that might be subject to other attacks. Each of the targeted organizations was running what appeared to be vulnerable web servers, but some were not seeing successful exploitation despite being sent phishing emails. For some organizations, there was no HTTP traffic seen in response, indicating that end-user training or email security solutions were likely preventing users from opening malicious emails. Other organizations did see responses consistent with users viewing the malicious emails, but no command and control beaconing was found after the fact.

These organizations may have been preventing successful exploitation by means of intrusion detection systems or anti-virus software, but Sally was unable to make a clear determination.

The reports created by Sally and her team provided a comprehensive view into the tactics, techniques and procedures that were being used by the threat actor. They also provided a potential list of other victims who LE could notify and provide mitigation and response recommendations. This ultimately resulted in the threat actors closing their operations and Sally's team seeing an overnight drop in malicious activity. The information from the reports was stored for potential use in identifying future campaigns and helping mitigate other threat activities.

Lessons learned

As Sally could attest, the lessons learned for preventing and mitigating servers from becoming C2 platforms for threat actors would include the following:

• Know threat actor tactics, techniques and procedures.

• Monitor file system changes on production servers.

• Operationalize monitoring.

• Conduct proactive reviews.

• Implement and review full packet captures.

• Watch for unexpected trends (e.g., SMTP from a domain server)

Incident management focus: Learning by waiting and observing

Dedicated threat actors often have the time and resources to play the long game and therefore will eventually compromise an environment if it is valuable enough. Both state-sponsored groups and criminal organizations have advanced capabilities and have been observed engaging in these types of campaigns. Despite different motivations, the results are the same: a formidable opponent for defenders. In cases such as this, it is often advantageous not to begin remediation immediately, but instead to monitor and assess the situation as a whole. Since remediating the vulnerability only solves the problem for the current instance, a determined threat actor will try again in a new way, from an unknown location. As such, the "devil you know" may be preferable to the one you don't, at least initially.

For LE, intelligence gained from operations such as this is invaluable. The ability to notify organizations of potential threats and share highly-targeted indicator information aids in situational awareness, which greatly reduces response timelines. Having access to this high-level view of what is targeted allows for better understanding of the goals and strategies of these advanced threats.

For organizations, the focus still needs to be on remediation (unless otherwise instructed by LE); however, care must be taken not to be overly hasty in these efforts. Threat actors may covertly compromise other systems to be used as redundant access points in case an IT Security Team patches the compromised system. In longer-term compromises, repurposing may have occurred and multiple types of malicious activity may be resident. The IT Security Team needs to understand the full scope of a compromise before attempting remediation so as not to tip its hand and cause the threat actors to go dark, only to reappear using hidden access methods months or years later.

Attack-Defend Card

CD-2: Mobile Assault – the Secret Squirrel

🛡 Breach scenario

Breach scenario
Indirect

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Confidentiality, Integrity

⌚ Incident pattern

Pattern
Crimeware, Cyber-espionage

Time to discovery
H — **D** — W — M — Y

Time to containment
H — **D** — W — M — Y

⚠ Threat actor

Composition
State-affiliated, Organized crime

Motives
Espionage

Tactics and techniques
Export data, Capture stored data, Exploit vulnerability

◎ Targeted victims

Industries
Professional, Administrative, Information, Manufacturing, Financial

Key stakeholders
Physical Security, Incident Commander, Legal Counsel, Human Resources

Countermeasures
CSC-1, CSC-3, CSC-13, CSC-15, CSC-17

Description
Mobile assault is an attack on devices directed at employees as they travel abroad. This can range from airport security personnel "holding your device" and extracting data, to hotel employees "swapping out hardware," to Wi-Fi hotspots set up as "rogue" access points to embed malicious software.

High-Value Targeting

Stakeholder

Endpoint Forensics Examiner

The situation

I love my job – it's constantly evolving and I'm always learning. As an endpoint forensics examiner and mobile device security expert, I not only have to keep up with numerous threats, but also a variety of platforms ranging from laptops to smartphones. I spend a lot of time chasing down "incidents," which often end up being nothing more than a problem between the chair and keyboard. Still, I wouldn't change a thing. As a part of the Verizon RISK Labs, I sometimes provide proactive forensics support to customers who have traveling executives that experience suspicious activity involving their digital devices. This requires me to find ways to secure and validate security on mobile devices.

> As an endpoint forensics examiner and device security expert, I not only have to keep up with numerous threats, but also various platforms ranging from laptops to smartphones.

After a recent trip, the Chief Security Officer (CSO) of one of our customers reported "odd behavior" on his smartphone. This description was a common one, usually fueled by paranoia mixed with jet lag; however, in this case, the traveling CSO was able to reproduce the unexpected behavior. He reported leaving the device in his hotel while he used the gym as well as connecting to a wireless access point in the coffee shop to save on the cost of a call home.

It was possible that all the suspiciousness was purely circumstantial, but in the name of due diligence, I collected his smartphone and laptop for processing. I hoped to find an obvious, albeit not serious, problem early on; otherwise, I would expect a long and difficult case. Proving a negative, especially in the face of reproducible problems, was not something I looked forward to doing.

Response and investigation

This organization was more prepared than most. Early on in the engagement, they requested we review their processes; based on our feedback, they had refined their travel security policy. As part of this refinement, their employees no longer traveled with their assigned corporate devices. Instead, they were given "travel" smartphones and laptops. After every trip, these devices were wiped and rebuilt. From a forensic examination standpoint, having this known baseline image to compare against drastically reduces analysis time and helps me focus on potential problems rather than background noise.

International travelers beware!

International business travelers frequently are forced to make security compromises when crossing borders. This can take the form of being required to connect to unfamiliar and innocuous Wi-Fi networks in order to access the internet. In other situations, users have to part ways with their laptop systems or smartphones at security checkpoints, and don't regain possession for what can be several critical minutes. Even more serious are those situations in which users are forced to decrypt their devices before handing them over for "screening examination."

We have long held the belief that a computer system that has left the user's possession for a significant amount of time – regardless of the security measures it has in place (e.g., encryption) – should not be fully trusted thereafter. Those who have access to devices from a logical or physical standpoint have an opportunity to compromise them in some fashion. As temporary custodians of mobile devices have access to more and more sophisticated means of compromising them, we will also need to evolve in terms of our methods of detecting deviances from "normal."

With forensic images of both the baseline images and the CSO's devices, I filtered out the known artifacts and produced a delta listing of items related to any changes. To help focus the search across this large set of data, I correlated the changes against listings of known indicators. These indicators, collected from previous engagements as well as open-source intelligence, included detailed file hashes, IP addresses, domains, and other signatures of known malicious activity. I knew these did not comprise a complete listing of all "bad stuff" on the internet, but it was a good starting point. I kicked off the search and took a break.

When I returned, I was met with a screen-full of results. Numerous Windows Registry changes and scheduled tasks had been identified on the laptop, each using known malware names. These file names were not unique, but they were not common enough to be an obvious false positive either. More unique keywords, such as domain names, were found in the local web cache on the smartphone. These domains were a strong indicator that malicious activity had taken place; however, they showed no signs of being related to the artifacts found on the laptop.

The Verizon Cyber Intelligence Center (VCIC) analysis revealed that the issues occurring on the two travel devices were indeed likely unrelated. Both showed signs of being opportunistic compromises rather than targeted threats. The application logs on the smartphone indicated that a third-party application, installed to avoid overseas call charges by using Wi-Fi and Voice over IP (VoIP), reported odd errors around the time of being connected to the public Wi-Fi. Research on the application revealed that it was known to be vulnerable to code injection attacks.

The laptop proved to be an even more opportunistic target with the web cache providing evidence of a drive-by download and injection from an advertisement displayed on a web page. Malicious Java files were found in the local directory pointing to an exploit kit used in broad attacks. It was very likely this laptop, when visiting the webpage in question, would have been affected even if it wasn't being used for travel.

Now that we had strong assurances that the laptop and smartphone – and by extension the traveling executive – had not been specifically targeted and were simply in the wrong place at the wrong time, I could focus on helping the customer remediate the issue and move forward. The devices were re-imaged to their baseline builds, and network and file system artifacts were loaded into security monitoring platforms to determine if other devices had been affected. Differences found between the forensic baseline and CSO images were provided to the customer for further review, allowing them to identify any sensitive information that might have been exposed.

Lessons learned

For this organization, preparation had prevented this minor breach from becoming a major incident. Their attention to detail when creating processes and procedures around travel not only mitigated the threat but also made validating the containment a trivial task. Despite the successful response efforts, the fact that a laptop and smartphone had been breached at all was a concern. An internal review determined ways to reduce the traveler-targeting risk:

- Provide employees with travel devices that can be rebuilt upon return; limit access from these devices and keep known baselines to expedite digital forensic review.

- Encourage travelers to note travel device usage times, locations, and other details including connections and accounts used.

- Train employees required to travel on proper device and data handling when abroad; provide resources related to country-specific legal concerns prior to travel.

- Do not grant employees administrative access to their devices; if admin access is required for job function, enact a policy restricting use or installation of non-approved third-party apps.

Attack of the killer BYOD!
Wipe, seize or deal with it ...

Employing a Bring Your Own Device (BYOD) policy can be a win-win decision for businesses. With corporate savings, employee convenience, and even the environmental benefits of reducing electronic waste, it is no wonder that more businesses are offering BYOD, with some even requiring it. However, businesses also need to consider the security ramifications that come with BYOD.

Business leaders must carefully weigh the risks versus rewards of allowing corporate data on an employee's personal device. A well-crafted BYOD policy helps protect business interests as well as facilitate an understanding with employees of their own risks. Some important considerations when developing a BYOD policy include the business' authority to seize or even wipe a personal device. Many businesses employ solutions that allow them to selectively wipe business data while leaving personal data intact. However, an important and often overlooked consideration is device backups.

An employee needs to have the freedom to back up their personal data, and in fact, many devices have built-in automatic nightly cloud backups. If corporate data is allowed to be backed up to personal cloud storage accounts, this puts sensitive data beyond the reach of the business. If the business decides there is a need to wipe an employee's device, the employee need only restore their device from a previous backup to regain access to deleted data. An additional aspect to be aware of is whether employees are creating unencrypted backups to their personal computers, which tend to be much more vulnerable to cybersecurity incidents.

Taking the overall situation into consideration, if you employ a third-party BYOD solution you may want to ask your vendor how you are protected when it comes to device backups and whether your employee is backing up data to the cloud or locally. Finally, consult with your Legal Department and the BYOD policy before wiping or seizing a device.

Mobile device forensic considerations

Mobile devices are designed differently than traditional computer systems. As such, they present many unique challenges when forensic images are required. Smartphones use various operating systems, which means there is no single solution for acquiring and analyzing mobile devices. Various tools may be required to acquire necessary data.

Part of the challenge is getting data from the device without performing "surgery" or causing irreparable damage. Many devices make the task even more difficult as they use encryption to protect the data at rest. Based on our experience, important considerations in dealing with mobile device forensics are:

1. **Properly isolate devices from networks.** This can be accomplished by disabling network connections, using a Faraday bag, or turning off the device.

2. **Have backup options to acquire the device.** If time is limited, know what type of data is required and choose the acquisition method(s) accordingly.

3. **Consider the volatility of evidence.** Essentially, there is no write-blocking for mobile devices. If the acquisition will occur immediately, do not turn off the device. If there will be delay or transport, turn the device off to minimize changes.

4. **Obtain legal authority to seize the device and collect the data.** This includes artifacts in the cloud, which some tools can collect.

5. **Do not blindly trust your tools.** Verify acquired data against the original device and manually review evidence sources to ensure that automated parsers present all available data.

Keeping the considerations mentioned above in mind during mobile device-related cybersecurity incidents will help with a smoother and more fruitful digital forensics investigation.
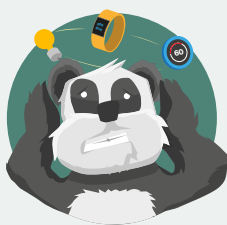
CD-3: IoT Calamity – the Panda Monium

Breach scenario

Breach scenario
Opportunistic (IoT Devices), Indirect (DoS Attack Victim)

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Availability

Incident pattern

Pattern
DoS attacks, Insider and privilege misuse, Crimeware

Time to discovery
H — D — W — M — Y

Time to containment
H — D — W — M — Y

Threat actor

Composition
Activist, State-affiliated

Motives
Grudge, Ideology, Financial

Tactics and techniques
Brute force, Privilege abuse, Scan network, Exploit vulnerability

Targeted victims

Industries
Entertainment, Professional, Educational, Administrative, Information, Manufacturing

Key stakeholders
Incident Commander, Legal Counsel, Corporate Communications

Countermeasures
CSC-1, CSC-3, CSC-9, CSC-11, CSC-12

Description
Security is often an afterthought when it comes to Internet of Things (IoT) solutions – and that means devices are often vulnerable to a wide array of threats. IoT calamity attacks take advantage of these cybersecurity shortfalls in IoT devices.

A Botnet Barrage

Stakeholder

Incident Commander

The situation

Senior members of my university's IT Security Team rotated weekly as on-call "Incident Commanders" in the event that a response was needed. This week was my turn and as I sat at home, my phone lit up with a call from the help desk. They had been receiving an increasing number of complaints from students across campus about slow or inaccessible network connectivity. As always seemed to happen, the help desk had written off earlier complaints and it was well after 9 PM when I was finally pulled in.

I joined the conference bridge and began triaging the information. Even with limited access, the help desk had found a number of concerns. The name servers, responsible for Domain Name System (DNS) lookups, were producing high-volume alerts and showed an abnormal number of subdomains related to seafood. As the servers struggled to keep up, legitimate lookups were being dropped – preventing access to the majority of the internet. While this explained the "slow network" issues, it raised much more concerning questions. From where were these unusual DNS lookups coming? And why were there so many of them? Were students suddenly interested in seafood dinners? Unlikely. Suspecting the worst, I put on a pot of coffee and got to work.

Response and investigation

Now that I had a handle on the incident in general, I reached out to the Verizon RISK Team, who we had on retainer, and began the process of escalating the issue. At their request, I gathered up network and firewall logs and passed them along for review. My IT Security Manager assured me that review would begin immediately and listed off a few of the triage steps he would be taking. All logs would be processed for known indicators of malicious activity and firewall logs in particular would be used to identify the sources of these requests.

Within hours, I had more feedback than I could handle and began the review process. The firewall analysis identified over 5,000 discrete systems making hundreds of DNS lookups every 15 minutes. Of these, nearly all systems were found to be living on the segment of the network dedicated to our IoT infrastructure. With a massive campus to monitor, everything from light bulbs to vending machines had been connected to the network for ease of management and improved efficiencies. While these IoT systems were supposed to be isolated from the rest of the network, it was clear that they were all configured to use DNS servers in a different subnet.

The impact of IoT

IoT possesses a huge potential to forever change the way we interact with our world through technology. The proliferation of IoT devices essentially leads to increased automation, big data analytics, and artificial-intelligence-based decision making in our daily lives. An IoT solution requires a detailed and comprehensive security and privacy framework — an area that unfortunately still requires a lot of work on design — as well as a substantial impetus on collaboration by the IoT market players on the underlying security.

Despite the fact that we are in a hyper-connected world, the security of the IoT is still at times somewhat of an afterthought. The main issue is that most firms do not realize that components behind the IoT's agile innovation can easily go wrong, and can have a far greater impact than what can be seen in the traditional IT landscape. IoT devices are usually constantly connected to the internet and may not be looked at from a security perspective, thus leaving them vulnerable to a variety of attacks. This makes IoT devices an ideal target for being conscripted into a botnet army.

The RISK Team provided me with a report detailing known indicators found in the firewall and DNS logs that I had sent over earlier. Of the thousands of domains requested, only 15 distinct IP addresses were returned. Four of these IP addresses and close to 100 of the domains appeared in recent indicator lists for an emergent IoT botnet. This botnet spread from device to device by brute-forcing default and weak passwords. Once the password was known, the malware had full control of the device and would check in with command infrastructure for updates and change the device's password – locking us out of the 5,000 systems.

This was a mess. Short of replacing every soda machine and lamp post, I was at a loss as to how to remediate the situation. We had known repeatable processes and procedures for replacing infrastructure and application servers, but nothing for an IoT outbreak.

> Short of replacing every soda machine and lamp post, I was at a loss as to how to remediate the situation.

Luckily, for me, a less drastic option existed than replacing all the IoT devices on campus. Analysis of previous malware samples had shown that the control password, used to issue commands to infected systems, was also used as the newly updated device password. These commands were typically received via Hypertext Transfer Protocol (HTTP) and in many cases did not rely on Secure Sockets Layer (SSL) to encrypt the transmissions. If this was the case for our compromise, a full packet capture device could be used to inspect the network traffic and identify the new device password. The plan was to intercept the clear text password for a compromised IoT device over the wire and then use that information to perform a password change before the next malware update. If conducted properly and quickly, we could regain control of our IoT devices.

While we waited for the full packet capture solution to be set up, I instructed the Network Operations Team to prepare to shut down all network access for our IoT segments once we had intercepted the malware password. Short lived as it was, the impact from severing all of our IoT devices from the internet during that brief period was noticeable across the campus – and we were determined never to have a repeat incident.

> The plan was to intercept the clear-text password for a compromised IoT device over the wire and then use that information to perform a password change before the next malware update.

Lessons learned

With the packet capture device operational, it was only a matter of hours before we had a complete listing of new passwords assigned to devices. With these passwords, one of our developers was able to write a script, which allowed us to log in, update the password, and remove the infection across all devices at once. The whole process took a matter of minutes and I made a mental note to save that script for later – although I prayed that we would never need it again. Now that the incident had been contained, we looked toward ways to prevent it from happening again.

Mitigation

- Don't keep all your eggs in one basket; create separate network zones for IoT systems; air gap them from other critical networks where possible.

- Don't allow direct ingress or egress connectivity to the internet; don't forget the importance of an in-line proxy or content filtering system.

- Change default credentials on devices; use strong and unique passwords for device accounts and Wi-Fi networks.

- Regularly monitor events and logs; hunt for threats at endpoints, as well as at the network level; scan for open remote access protocols on your network and disable commonly unused and unsecured features and services (such as Universal Plug and Play (UPnP) and Real Time Streaming Protocol (RTSP)) that aren't required.

- Include IoT devices in IT asset inventory; regularly check manufacturer websites for firmware updates.

Response

- Develop and follow your pre-designed IR playbooks to tackle IoT device-related incidents.

- Scope and contain incident immediately; segregate affected subnet and restrict network ingress and egress communication to/from affected subnet.

- Change admin or console passwords of the IoT systems and controllers.

- Leverage network forensics, to include network logs, NetFlow data, and packet captures.

- Consider informing Law Enforcement (LE) and regional Computer Emergency Readiness Team (CERT) organizations as egress communication may have impacted other entities and the related threat intelligence could help other potential victims.

The evolution of the IoT

Like any typical Gen-X technology, the IoT continues to evolve and has gone through a growth spurt over the past few years. This rapid proliferation has led to as many new issues as the underlying devices were intended to solve.

The underlying problem is that many IoT manufacturers are primarily designing their devices for functionality; and proper security testing often takes a back seat. It's even more necessary with IoT devices that the buyer scrutinizes the security of any devices they use. IoT botnets spread quickly because they don't face some of the problems conventional botnets do, due to the fact that IoT devices are often rarely patched or updated.

In addition, the vendors that create IoT devices, along with the users that own and operate them, aren't always directly impacted by a compromise or even immediately aware that their devices played a role in a cybersecurity incident. In a number of these circumstances, the IoT environment leveraged in an attack is not actually the intended victim, but rather an involuntary accomplice that is being used to attack an unrelated third-party target.

IoT threats go well beyond a typical security breach where concerns revolve around the theft of confidential data. In this new age of IoT breaches, we are seeing a growing and wide-ranging impact in our physical world as well as on human life/safety (e.g., transportation or medical device incidents) and even a changing financial and legal liability landscape.

Today, the IoT is not confined within an organization's typical control boundary, as the connected infrastructure has moved far beyond those control lines. These devices exist virtually everywhere, are available anytime, and are on a variety of platforms. This must prompt organizations to think about IoT threat modeling in a manner that incorporates security and privacy by design.

CD-4: USB Infection – the Hot Tamale

Breach scenario

Breach scenario
Specific

Sophistication level
1 — **2** — **3** — **4** — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Insider and privilege misuse, Crimeware, Cyber-espionage

Time to discovery
H — **D** — W — M — Y

Time to containment
H — **D** — W — M — Y

Threat actor

Composition
Other (Employee), Organized crime, State-affiliated

Motives
Financial, Espionage

Tactics and techniques
Unapproved hardware, Spyware/ Keylogger, Backdoor, Exploit vulnerability

Targeted victims

Industries
Accommodation, Financial, Manufacturing

Key stakeholders
Physical Security, Human Resources, Legal Counsel, Incident Commander

Countermeasures
CSC-1, CSC-3, CSC-6, CSC-16, CSC-19

Description
USB devices, and other portable media, represent a significant threat to organizational security. Threat actors with physical access can introduce toolkits, built to run directly from the USB device itself, to bypass access controls. Employees curious about content on USB devices can also introduce malware to their work systems.

The Dirty Cleaner

Stakeholder

Internal Investigator

The situation

Contractors, such as auditors and janitorial staff, can often be nearly invisible in large corporate environments. It is said that one can get nearly anywhere with a purposeful stride or a handy prop of authority, such as a clipboard or a mop. Depending on their role, contractors may also have access to broader and more varying areas than your typical employee. That's why a contractor who is given an economic or vengeful incentive can become a potent threat vector.

> It is said that one can get nearly anywhere with a purposeful stride or a handy prop of authority, such as a clipboard or a mop.

Most employees have little awareness of business operations changes with vendors, service providers, or contractors. These details are hidden away inside Human Resources (HR) and Accounting departments focused on keeping the company running. Therefore, it was no surprise that neither I, nor the rest of the IT Security Team, had any idea of the problems brewing with our contracted janitorial service. The contracting company had announced a unilateral pay cut for all employees and chose to reveal this information mere weeks before the holiday season.

> The task was easy: Simply carry a USB flash drive in each day and then get paid for each system it was plugged in to.

Even had we been aware of these contracting changes, no one would have guessed that the now emotional and desperate janitors would be approached by a malicious individual offering them "bonus pay." The task was easy: simply carry a USB flash drive in each day and get paid for each system it was plugged into. Feelings of retribution toward the contracting company mixed with the financial strain on employees turned out to be enough to convince more than one janitor to accept the cover story.

The janitors, hidden in plain sight, had access to everything and were able to quickly compromise multiple systems without arousing suspicion. The infected systems would likely have remained hidden for weeks or months had an eagle-eyed administrator not noticed unexpected command shell pop-ups upon logging in. A brief investigation showed these tasks running under a local administrative account and did not seem to be related to any legitimate business activity. After adding a few notes to a trouble ticket, he clicked send, and then carried on to other tasks.

Incident pattern: Cyber-espionage

For cyber-espionage, the objective is specific and the digital footprint is kept to a minimum (and in many cases, attempts are made to cover the tracks and erase the footprint). Nothing is smashed or grabbed (as in most point of sale attacks). Credentials are collected. Access is increased. And it all occurs slowly, covertly, and deliberately, until all corners of the victim organization have been compromised. The compromised victim might not even be the ultimate target of the threat actor, but instead may serve as a springboard for entry into a larger organization with which the victim may have a trust relationship.

Once they are finally discovered, these breaches require a great deal of care to mitigate. The corporate network may no longer be trusted (since all domain credentials are assumed compromised), so out-of-band communication channels must be established as remediation plans are put in place. Finally, a date is set at which point the old domain is retired and a replacement must be built from the ground up, including establishing new credentials for every user.

Response and investigation

This is where I come in. As an internal investigator, I'm tasked with figuring out what this type of stuff means. Are these system artifacts malicious? Are they left over from previous configurations? Ultimately, how did this stuff get there? These were the questions my organization wanted me to answer.

The first order of business was to establish a footprint of systems affected by the attack. This list would help guide me toward determining the initial vector of the infection. Having met with the IT Security Team to understand the "weird stuff" observed, I started pulling domain and system logs from the initially identified workstation. These "weird things" are what we traditionally refer to as Indicators of Compromise (IoCs), and are the bread and butter of locating additional systems affected by a known piece of malware. Searching through the domain logs with these IoCs in hand, I was able to quickly identify several other systems, each of which had been accessed by the same local administrator account within the same timeframe as the suspect system. This correlation expanded the scope of the investigation to include additional systems beyond the one originally anticipated.

> The first order of business was to establish a footprint of systems affected by the attack. This list would help guide me toward determining the initial vector of the infection.

With the larger list of systems enumerated, I presented my preliminary findings to our HR Team and Legal Team and identified various options. The decision was made ultimately to call in the Verzion RISK Team to conduct digital forensic analysis on the system in question, and determine, to the extent possible, the nature of the malicious activity. The RISK Team soon arrived on site and forensically imaged the in-scope systems. These images were then subjected to multiple types of review, ranging from analysis of the Windows Registry hives to examining system log files and reviewing the shortcuts for suspicious linkages.

The analysis of the systems logs revealed suspicious command line activity and exploitation attempts, as well as subsequent, unsuccessful clean-up attempts. Interestingly, these same logs showed a USB device driver being loaded onto the system just prior to these exploit attempts. Based on serial numbers found in the Windows Registry as well as other artifacts, it was determined the USB device was a cheap flash drive indistinguishable from dozens of others.

In our organization, there has always been an official policy against such devices being used, but it was rarely enforced with employees. The problem with USB devices in corporate environments is that once a device is plugged into a system, it could force system configuration changes or allow unauthorized programs to run. This could then allow a whole host of other actions to occur on a system. This potential threat tied with the suspicious timing raised a red flag in my mind and merited further review.

At this point, an artifact showed a USB device had been connected to the system, but a primary question remained: who connected it? Armed with date-time stamps relating to the USB device driver being loaded, I met with the team responsible for overseeing the physical security of the company campus. I was hoping that we might be able to track who had physical access to the system during the relevant timeframe. To my elation, they informed me that they required badge access to the room where the in-scope system was located.

As you can imagine, I was anxious to see these logs! After a short time, the Director of Physical Security was able to produce all the badge access logs for me. I found there was not a lot of access to that room around the time the USB device activity was identified on the system. The only thing that stood out was the janitorial staff doing their cleaning rounds at that time. It took me a few passes but eventually I had my "Aha!" moment. Could a janitor be my primary suspect? Might they have been plugging something into that workstation? Or others? I thought we'd better ask.

Our HR Department and Physical Security Team interviewed the janitor concerned, and they admitted to plugging the USB device into multiple systems. These systems and timeframes matched identically with my log review and the RISK Team analysis results. With the technical portion of the analysis complete, I was able to sit back and watch as our HR Department continued to interview the janitor. They expressed remorse, but explained that the upcoming pay cuts would have caused extreme difficulty for them. The prospect of additional holiday spending money and a lack of understanding about the potential for damage led them down a path they couldn't reverse.

Lessons learned

The janitor was terminated ultimately and the exploit attempts ceased. Further review indicated that this activity was caught quickly enough that the threat actor never managed to locate or extract privileged information. Remediation was limited to increased monitoring of IoCs and cleaning up the affected systems. Future mitigation was implemented by logging and centralizing hardware device changes across all sensitive or restricted systems.

While there were digital components to this breach, the biggest takeaway is the importance of physical security. It's well known that direct access to a device circumvents many security controls. Access to USB ports may allow bad actors to load malicious software just as easily as a device can be rebooted in safe mode or have its drives removed to bypass password security. The following represent technical and physical considerations to make before and during this type of suspicious activity:

Mitigation

- **Establish host-based USB device access/antivirus policy.** Having host-based enforcement limiting USB device port access could have stopped this attack before it even began. Certain company-provided devices could be whitelisted so as not to entirely remove the functionality. Furthermore, host-based anti-virus can be employed to scan any media that is newly connected to a workstation or device.

- **Disable auto-run functionality.** IT Teams capable of remotely updating system configurations should disable auto-run on non-affected systems to limit the potential spread of USB-based infections.

- **Enhance host-based logging and alerting.** If it wasn't for the vigilance of a systems administrator, this security incident may have gone unnoticed long enough to inflict serious damage to the company. The physical vector also creates very little network noise in which similar activity is usually discovered. In this case the logs were present for systems; however, there was no alerting functionality to trigger on suspect activity.

- **Leverage network access controls.** In this scenario, the adversary was defeated early in the reconnaissance and lateral movement stage. However, our company employs a relatively flat network design, which means that systems may have expanded network accessibility to sensitive systems. Implementing network access controls made it harder for an adversary to use less secure systems to compromise more secure systems.

- **Set up physical access alerting.** Access cards allowing limited access to certain areas secure many offices. However, it is trivial for a card to be lifted off a desk or cloned with a proximity reader. Alerts were set up and monitored to look for consistent access patterns, such as an employee badge being used several hundred feet from their last scan within a short timeframe.

- **Limit local administration accounts.** While local administration can be convenient for help desk and power users – it opens a vector that can be harder to monitor. Domain admin accounts allow for better security auditing and alerting. We also used various solutions for granting temporary local administration privileges to assist in day-to-day troubleshooting and installs.

Response

- **Review physical security access controls.** Badge readers, security cameras, and sign-in logs should not be ignored; these can reduce suspicious user activity requiring investigation.

- **Use endpoint detection and response solution to identify affected system.** Once an affected system is identified, disk forensics paired with an Endpoint Detection and Response (EDR) solution can allow a direct view into additional systems that may be affected.

- **Review network and application logs.** Review logs related to compromised systems or user accounts to determine other assets which may be been targeted.

- **Conduct personnel interviews.** Interviewing employees, contractors or other people with access to affected devices can help identify suspicious behavior. Additionally, these interviews may uncover "weird" or otherwise unexpected events on affected systems, which can act as investigative leads for forensic investigators.

Incident management focus: Investigative approach

Management of cybersecurity incidents is a crucial part of a business's security strategy. For that reason, companies invest heavily in the creation of a customized corporate Incident Response (IR) Plan. In many cases, this is not a one-time investment and they continually re-invest in maintenance of this living document and continued training to enable a quick recovery from a cybersecurity incident. This additional diligence not only aids in maintaining compliance, but also provides a robust foundation for protecting corporate interests from cybersecurity-related threats. As part of the incident management process, defining investigative approaches for predefined security incidents based on known potential issues can improve IR efforts.

A well-defined investigative approach can decrease the time required to resolve a cybersecurity incident while increasing the reliability of actionable evidence. By defining the tools and the steps to be followed, analysts can work faster as they follow the same procedures while not wasting time considering what steps to take next. This can reduce the chances that the analyst will forget to run a tool or look for specific evidence. Greater efficiency can be built into the investigative process by running programs, which have longer processing times at the beginning of an investigation, allowing the analyst to continue working while those tools are running.

In addition to efficiency, in an environment where multiple analysts may be working on individual cases or together on a joint case, following the predefined investigative approach grants continuity in the investigation allowing one analyst to pick up where the other one left off. If at some point an investigation is called into question, being able to show that the analyst followed the same steps for previous investigations lends to the credibility of the process. A well-defined investigative approach has many benefits; however, it is also important to have leeway in the approach to permit analysts some degree of freedom to follow their instincts.

Configuration Exploitation

Configuration is a part of every network schema, hardware device (firmware), and software application. Proper configuration can prevent or mitigate threat actor activity while weak configurations are prime targets for threat actors and their vulnerability exploits.

From a system standpoint, misconfigured devices are the vectors of compromise; from a network standpoint, misconfigurations allow for easy lateral movement and avenues for data exfiltration.

Configuration is a part of every network schema, hardware device (firmware), and software application. Proper configuration can prevent or mitigate threat actor activity while weak configurations are prime targets for threat actors and their vulnerability exploits. From a system standpoint, misconfigured devices are the vectors of compromise; from a network standpoint, misconfigurations allow for easy lateral movement and avenues for data exfiltration.

Often the weakness leveraged by the threat actor to gain access to a device is one solved not with a patch, but with adjustments to existing configurations or architecture, such as leveraging file upload capabilities to upload web shells, open Remote Desktop Protocol (RDP) sessions to the internet, and other malicious actions. And while it is impossible to gather statistics on "weak configurations" as a whole, we do have statistics on the number and frequency of breaches involving attacks against single factor authentication. Almost half (46%) of organizations breached as seen within the VERIS data over the previous three years involved the use of stolen credentials or brute force attacks/password guessing.

Scenario CE-1 (Website Defacement) describes a website modified by threat actors to bring negative attention to the victim organization, while Scenario CE-2 (DDoS Attack) describes a four-pronged Distributed Denial of Service Attack (DDoS) by a known hacker group. Scenario CE-3 (ICS Onslaught) describes outdated Operational Technology (OT) systems that were targeted by hacktivists. Scenario CE-4 (Cloud Storming) covers a compromised e-commerce site, which resulted in the exposure of sensitive customer data hosted in the cloud.

Security imperative: Web application firewalls

Web application firewalls, or WAFs, provide an additional layer of security for web applications by inspecting and blocking traffic based on protocol-specific rules. Like many of the traditional firewalls, WAFs allow for blocking traffic based on source IP addresses, destination file, or directory paths, but are also capable of inspecting Hypertext Transfer Protocol (HTTP) traffic in ways commonly associated with an intrusion detection or prevention solution. These advanced features allow web administrators and developers to safeguard against common vulnerabilities such as cross-site scripting or Structured Query Language (SQL) injection.

Web application firewalls come in many forms ranging from vendor-provided hardware appliances to open-source, free software, and cloud-based solutions. Appliances are frequently agnostic of the underlying web server technology and operate in-line, detecting and, when configured properly, preventing attacks. Software-based firewalls are usually paired with a specific HTTP daemon, such as Apache or Windows Internet Information Services (IIS).

Configuring a WAF is the most critical and often the most time-consuming step in a deployment. Default rules exist for most solutions; however, highly customized or complex web applications may require default configurations to be overridden to function properly. Certain rules may interfere with core functionality of the protected applications and a decision must be made whether to modify the WAF's configuration or to update the application's code.

When paired with well-designed, secure applications, WAFs act as a defense-in-depth strategy to mitigate programmer error or unknown problems. Applications designed with security in mind are more resilient to attack, but it is unreasonable to expect developers to account for every possibility. Even when a WAF does not prevent an attack, it typically logs at least some suspicious activity, which can be helpful when correlating with other forensic evidence sources.

CE-1: Website Defacement – the Hedley Kow

🛡 Breach scenario

Breach scenario
Specific (Hacktivist Attack), Indirect (Vulnerability)

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Confidentiality, Integrity

🕐 Incident pattern

Pattern
Web application attacks

Time to discovery
H — D — W — M — Y

Time to containment
H — D — W — M — Y

⚠ Threat actor

Composition
Activist, State-affiliated

Motives
Ideology, Grudge, Financial

Tactics and techniques
Use of backdoor or C2, Brute force, Privilege abuse, Exploit vulnerability

◎ Targeted victims

Industries
Financial, Retail, Information, Administrative

Key stakeholders
Incident Commander, Corporate Communications, Legal Counsel

Countermeasures
CSC-3, CSC-4, CSC-6, CSC-16, CSC-18

Description
Although not a data breach per se, website defacements can seriously impact a corporation's public reputation. Losing control of communication channels, such as websites, social media accounts and advertising, allows threat actors the ability to broadcast anything they wish.

Digital Graffiti

Stakeholder

Corporate Communications

The situation

It's kind of funny if you think about it. Two weeks prior to the incident, I sat in a boardroom with the CEO, General Counsel, Human Resources Director, CIO, CISO and Dan, our newly hired IT Security Team member, running through an Executive Breach Simulation (EBS) run by the Verizon RISK Team. I manage the Corporate Communications Team for a large media firm and I was adamant about being involved with the response to any serious cybersecurity incident. I felt strongly that I was more than just a good point of contact when someone needed to get a message out to the media. My skills could also be a tremendous asset to the company during times of crisis, too. The CEO agreed and was insistent that I attend the EBS. Little did we realize that the cybersecurity response procedures we were rehearsing and the issues that we were discussing would soon be put to the test in a real-world situation.

Dan, being the new IT security guy, often found himself stuck with the graveyard shift. This particular Friday night was shaping up to be pretty normal for Dan; a light amount of work mixed in with studying for an upcoming IR certification. As Dan was reading through his course material, he heard a notification from his email client that a high priority message had been received. Quickly switching tasks, he opened the mail to find that a number of public-facing client websites showed modifications to their content. Checking the change management schedule, Dan verified that no planned updates had been deployed to any of the affected sites. He pulled up the IR Plan and ran through the checklist to notify all those involved in the EBS, including the RISK Team.

Incident pattern: Web application attacks

Attacks on web applications are not a new trend; hackers have been targeting websites since the early days. Originally, web applications were compromised and defaced, a form of digital graffiti, to show the prowess of a hacker or group of hackers. As our world became more internet-connected and web applications began hosting retail and financial transactions, the motivation to attack them changed from vanity to greed. We still see occasional hacktivist-type activity where spreading a message through defacement occurs, but the vast majority of attacks on web applications are financially motivated.

Web applications compromised for data rather than defacements can be much more difficult to identify, much less resolve. Defacements make obvious the presence of unwanted content, whereas backdoors or infections silently stealing data can remain hidden for months or years. Detecting a covert compromise may require the use of file integrity monitoring, detailed and accessible application logging, or reviewing inbound and outbound connections involving web servers and suspicious IP addresses.

Luckily, preventing covert compromises shares many of the same to-do items as preventing a website defacement. Applications should be built using a development life cycle, which has designing secure applications at its core. Validation should be done on new or updated applications to check that all inputs are properly sanitized and access controls still function effectively. A web application firewall or intrusion detection platform can be added in front of the web servers to act as an early warning and prevention system. Finally, applications need regular monitoring and updates post-release to help keep unknown or anomalous activities from occurring.

Response and investigation

When I arrived in the "war room" later that evening, Dan was busy on the phone with the RISK Team providing all sorts of information while my attention was focused on the media response. By the time I arrived, Dan and the RISK Team had already ruled out a number of initial hypotheses. The threat actors did not appear to have compromised any account credentials nor had they apparently had access for very long. The in-place monitoring solutions only alerted changes on public-facing pages; a file review on the affected web servers revealed modifications and uploads going back only a few days.

> The in-place monitoring solutions only alerted changes on public-facing pages; a file review on the affected web servers revealed modifications and uploads going back only a few days.

The RISK Team continued to work through the data relaying information and questions back to Dan for follow-up and validation. Each affected site, while containing a different defacement, showed many similar characteristics when other modified files and log entries were compared. It appeared that whoever had gained access to one site had used a consistent methodology to compromise the others. Our web application framework was highly customizable through an extensive configuration file, which allowed enabling of features, modifying of behaviors and the creation of unique input forms. If someone was compromising multiple sites in similar ways, odds were good that there was some underlying problem with this application. The configuration file comparison revealed that only newly deployed applications were affected, with nothing created prior to the most recent code release showing signs of compromise. Not all new sites had been compromised, but no older sites appeared to be part of the incident.

In the most recent change, an update to how the installation scripts initialized the environment had been included. This change was designed to allow for additional flexibility in applications, which leveraged custom fields. However, the feature had been enabled by default in all new installations due to a forgotten debugging option left by a developer. The RISK Team's analysis revealed that, if enabled on sites not leveraging custom fields, this option bypassed input validation features and ultimately allowed the threat actors to upload malware.

The technical remediation was assigned to Dan and he spearheaded an effort to get correctly updated code pushed to production, to begin rebuilding the affected websites, and to validate that the defacement was the only malicious activity present.

The messages posted to client websites for more than 24 hours were inflammatory and extremely negative, which cast each client in an extremely bad light. While no data had been stolen and the compromise was quickly handled, affected clients wanted answers on how this would be prevented in the future. After the EBS that we had conducted a few weeks prior to the incident, I had started an initiative to conduct research on external Public Relations (PR) firms and select one as a partner to assist us in situations like this. At the time of the incident, we had selected a firm, but had yet to formalize the arrangements. The incident helped accelerate the necessary contractual reviews. However, we were not able to obtain signatures until late in the incident – around the same time that the engagement was winding down – so we didn't end up leveraging our new partner as much as we originally anticipated.

> The messages posted to client websites for more than 24 hours were inflammatory and extremely negative, which cast each client in an extremely bad light.

Our CEO prides herself on being upfront with customers and, in this cyber emergency, she made it clear that our response to any client impacted by this incident should be as open and honest as possible. As we began to compile a list of impacted clients, we brought in our client relationship managers and crafted a plan to reach out to each client individually. I drafted a formal statement that we would send to each client, as well as capturing key talking points for discussions with customers. We anticipated that any written statement or letter sent to customers would make its way to the media, so we formulated a strategy to deal with any media attention drawn to this incident.

> We anticipated that any written statement or letter sent to customers would make its way to the media, so we formulated a strategy to deal with any media attention drawn to this incident.

In parallel with the external communication strategy, my team started crafting an internal communication to all employees to inform them of the incident. Our websites had been defaced and this was already public knowledge. However, we needed to ensure our own employees knew that we were on top of the problem and were developing a strategy to contact impacted clients. We also took the opportunity to remind employees that they should not speak with anyone outside the company, which included clients, media, family, friends, etc., regarding the incident. All inquiries were to be directed to my team immediately.

Throughout the IR process, I had remained closely engaged with Dan and the technical teams to ensure I understood the facts. I am not a technical person, but with a little help and patience from Dan and the CISO, I was able to understand most of the technical details surrounding how the websites were defaced. Participating in the IR process from the beginning and seeing events unfold was invaluable to my understanding of the facts. This directly enabled me to accurately convey information to our customers.

In the end, we sent letters to several hundred customers impacted by the website defacement, and our CEO made herself available to speak individually with over a dozen impacted clients. To our customer base, this sincere and direct approach proved invaluable in providing them the assurances they required and we were able to minimize the impact to our business.

Lessons learned

Practicing our IR Plan during the recent EBS was a major factor in running this incident smoothly. Having the Corporate Communications Team on site during the response activities was vital to getting a solid message out to protect the reputation of our business. Lessons learned included:

- Develop a strategy to handle media inquiries; be able to rapidly scale up Call Center operations to handle inbound inquiries.

- Prepare templates for customer notifications; adjust as necessary for the situation.

- Have clear and concise internal communications with all incident stakeholders; funnel all internal communications through the IR and Crisis Management Coordinators.

- Keep the Board of Directors informed of progress, results, and post-incident activities; and regularly update all stakeholders on the progress, findings, and actions yet to be taken.

- Be as transparent and timely as possible by notifying impacted customers, given the circumstances and local regulations/statutes.

- Remind employees of the corporate policy prohibiting speaking with reporters, and direct all inquiries to the Corporate Communications Team.

In terms of technical mitigation and response recommendations, the items discussed in the incident after action review included:

Mitigation

- Review code and configurations.

- Conduct security and application scans.

- Update management processes to include testing.

- Keep applications and server platforms updated.

- Install and configure a web application firewall as per best practices.

Response

- Restore from known backups or rebuild affected systems.

- Patch or update identified issues.

- Block offending IP addresses.

- Prepare public relations response to content.

- Verify that quality assurance process catches configuration issues.
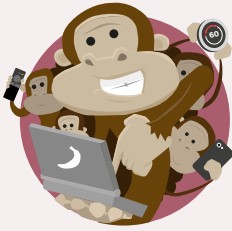
CE-2: DDoS attack – the 12000 Monkeyz

Breach scenario

Breach scenario
Specific

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Availability

Incident pattern

Pattern
DoS attacks

Time to discovery
H — D — W — M — Y

Time to containment
H — **D** — W — M — Y

Threat actor

Composition
Activist, State-affiliated

Motives
Grudge, Ideology, Financial

Tactics and techniques
Brute force, Privilege abuse, Scan network, Exploit vulnerability

Targeted victims

Industries
Entertainment, Professional, Educational, Administrative, Information, Manufacturing, Retail

Key stakeholders
Incident Commander, Corporate Communications, Legal Counsel

Countermeasures
CSC-3, CSC-9, CSC-11, CSC-12, CSC-19

Description
A Denial of Service (DoS) attack involves a single computer using its network connection to flood a targeted system or resource with traffic. Distributed Denial of Service (DDoS) attacks leverage large numbers of systems to disrupt network operations across large networks.

No Patch,
No Service

Stakeholder

SOC Analyst

The situation

DDoS attacks seem to be climbing at a steady rate year over year. The motivations for such attacks range from disrupting hostile competition, extortion, and political objectives. Although the incentive to launch a DDoS is rarely exfiltration of data, disruptions of a service or product can be just as devastating for any business. With the rise in popularity of DDoS attacks for threat actors, toolkits to launch these attacks have become easier to use and more effective by increasing overall bandwidth capabilities. Preparations for a DoS or DDoS attack include having the right team to handle the situation and is a critical component of the mitigation and recovery phases when dealing with these types of attacks.

> With the rise in popularity of DDoS attacks for threat actors, toolkits to launch these attacks have become easier to use and more efective by increasing overall bandwidth capabilities.

As a Security Operations Center (SOC) analyst, the ability to leverage tools and resources – in-house, external, or social media – definitely helps defend against some of the most aggressive attacks during pivotal times for the business.

During one of the largest volumetric attacks against a company in the software-as-a-service sector, I stood in the front lines of an uphill battle that exhausted all response team resources. Ultimately, this event shaped the way product launches and security were handled in the future for the company.

We determined the objective of the threat actor was solely to disrupt a holiday week and, in doing so, deny clients access to tools essential to handling their holiday workload. This well-timed attack coincided with a new product release date and a week in which a substantial influx of users was expected. Thus, the attack against our bandwidth would be compounded with tens of thousands of legitimate users trying to connect simultaneously.

With an attack of such great magnitude, the identifiers came in various forms – NetFlow graphs showed a 300 percent increase in the sample; Top Talkers lit up the target prefix to which most of the traffic was destined; and point-to-point protocol (PPP) Generic Routing Encapsulation (GRE) tunnels started to bounce up and down due to oversaturation. As a result, some applications were inaccessible to users wishing to access their accounts.

Our capability to view network traffic live with packet analysis tools played a major role in the active mitigation process. Review of the collected packets revealed four distinct types of DDoS: A Simple Service Discovery Protocol (SSDP) flood; a SYN flood; a Transmission Control Protocol (TCP) flood using invalid flag combinations; and a User Datagram Protocol (UDP) flood to non-web ports.

With so many types of DDoS, the priority for me as a SOC analyst was to mitigate what I could and attempt to recover the systems to a usable state. While the rest of the SOC and I worked to deal with the issue, the Verizon RISK Team was tracking the source of the threat actors, and investigating the extent of the threat actor's actions.

Response and investigation

One of the major challenges my organization dealt with when responding to the attack was routing the flood to our DDoS mitigation provider. When the DDoS attack occurred, we found our IT team underprepared and unable to quickly adjust our publicly advertised border routes. Initially, the routes were added to pass traffic through a scrubbing service prior to being sent to our servers; however, without clear documentation the engineer making the changes left the existing routes in place. This small oversight allowed roughly half of the incoming traffic to bypass the DDoS mitigation provider. After a tense hour diagnosing the problem, we discovered and corrected the error allowing us to move on to other forms of mitigation.

> Most of these systems were compromised routers running old firmware with UPnP enabled; odds were that many of these were "NYP'd" (not yet patched).

With the proper routing in place, we were able to begin handling the discrete attacks. Source-to-destination Access Control Entries (ACEs) were used to mitigate most of the SSDP and Invalid TCP flag combinations. This single action reduced a large portion of the attack traffic; however, considering the overall size of this attack there was still work to be done.

The non-spoofed IP addresses were reviewed and it was revealed that each had an open SSDP port (1900), which was publically accessible from the internet. Most of these systems were compromised routers running old firmware with Universal Plug n Play (UPnP) enabled; odds were that many of these were "NYP'd" (not yet patched). This was not an uncommon situation. On any given day, there are millions of systems on the internet, which would respond to a network scan with the port shown as open. These types of systems are perfect targets to become zombies for hackers to leverage and amplify an attack.

The three-part handshake

Applications that require reliable communications often leverage protocols built on the Transmission Control Protocol, or TCP. To achieve high levels of reliability, TCP uses a variety of control flags to communicate the state of a connection and validate receipt of data sent across a connection. When analyzed, these flags can provide valuable insight into network behavior, and be used to understand the nature of any malicious communications.

A core component of TCP is the "three-part handshake," a mechanism used to validate that both hosts involved in a communication are aware and ready for data transmission. To initiate a connection, the requestor, or client, sends a TCP/IP packet to the requested host, or server, containing a single flag. This SYN flag asks the server to SYNchronize with the client. If the server agrees it will reply with a two-flag packet, SYN-ACK, as a way of both ACKnowledging the synchronization request as well as asking the client to synchronize with the server. If the client is still willing to participate in the communication it replies with a final single-flag packet, ACK, to let the server know the client is ready for further communications. Once the full handshake (SYN, SYN-ACK, ACK) has been completed, the two hosts may transmit data bi-directionally for as long as timeouts allow.

For a security analyst the TCP handshake can be a valuable way to quickly verify the state and legitimacy of network communication. When dealing with infected networks, we must frequently filter through large amounts of network traffic to identify potentially suspicious or malicious communications. One way in which connections can be eliminated, thus reducing the data corpus to review, is by searching for communications, which show only a full three-part handshake.

TCP sessions identified without these exact packets have a very low probability of data transfer, and therefore are unlikely to contain malicious activity or exfiltrated data. This is especially the case with DDoS-related attacks. Abnormalities in the handshake pattern or missing final ACK packets can be strong indicators of forged, or spoofed, traffic. In the case of highly segregated environments, even unsuccessful connections may be suspect and these flags can be used to triage types of traffic for later review.

Mitigating the UDP flood proved more difficult as it was destined for a port that this customer relied on for normal application traffic. Denying traffic to the UDP ports with a blanket statement would have also denied the legitimate user base. The threat actors knew exactly where to focus their attacks. Mitigation for the UDP flood had to be handled by an appliance, which would scrub the traffic in line, and subsequently drop packets that were not defined within the rule set parameters. A custom mitigation rule was created to match the payload signature, packet size, and destined port.

The SYN flood was also handled by a mitigation appliance, but would instead challenge incoming TCP connections. Spoofed source IP addresses wouldn't respond to the challenge and would be dropped. Legitimate user connections would reply successfully and make a full TCP connection. This particular mitigation strategy is effective but can cause collateral damage since there is no way of proving a user is legitimate without going through the same challenge mechanism in order to authenticate.

During the investigation, the RISK Team identified a known hacking group that was using the DDoS as a way to advertise their services. The threat actors stated that for a nominal Bitcoin fee, they could bring down any other application for an extended timeframe.

With the full mitigation stack in place, the DDoS attack's effectiveness subsided and services were restored eventually. As a result of the attack — and learning several hard lessons — my company was ultimately able to improve its overall security posture. Large-scale DDoS attacks can't fully be prevented, but having the right resources to battle them can drastically reduce downtime and hasten recovery.

Recommendations to add permanent Access Control Lists (ACLs) for incoming TCP connections were put in place. These entries followed a Request for Comment (RFC) standard for TCP flag combinations, and would drop invalid flag sets immediately without making it through the GRE tunnel and ultimately hitting the backend, which lies further downstream. The same recommendations were made for the UDP traffic. Unexpected ports would be dropped upstream and only legitimate destination port ranges would ever be allowed. Although this may seem like standard practice, networks change constantly and sometimes drastically and therefore should always undergo rule revisions.

In addition to adding traffic rules for inbound connections, the frequency of service validations and mock incident tabletop exercises were increased to every quarter. Having the capability to run a standard attack scenario every three months, without the same pressures of an actual attack, was now part of the standard regimen for all teams. These exercises allowed kinks to be worked out in a controlled environment.

Lessons learned

As the number of DDoS tools, IoT devices, and misconfigured systems increase, a security regimen that considers large-scale attacks is paramount. Having a strong security posture and remediation plan can drastically reduce downtime and hasten an organization's ability to respond and recover. Organizations would do well to consider the following baseline plan of action:

Mitigation

- Automate prefix routing to the DDoS provider and test the functionality periodically.

- Funnel advertised routes as intended.

- Increase bandwidth to essential networks.

- Use well-defined ACLs and firewall rules.

- Limit (half-open) connection rates.

Response

- Validate services to rule out unexpected complications during an attack.

- Conduct post-incident investigations.

- Conduct social media awareness campaigns.

- Document processes for handling DoS attacks.

It is vital to take a proactive approach to defending your network especially when your customers are using it. In these circumstances, additional security enhancements, like those listed in this exercise, can significantly reduce downtime for these types of attacks. Although it is a best practice not to engage an attack group, it is always advisable to keep an eye on social media feeds. Threat actors may brag about taking a company down or hint at attempting to do so. Any potential precursors to an impending attack will certainly reduce the element of surprise.

Incident pattern: DoS attacks

Denial of Service (DoS) attacks are any attack intended to compromise the availability of networks or systems. This includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service. According to VERIS, top industries we see targeted are online gaming, information technology services and financial institutions. While this technique is available to a broad range of threat actors, DoS attacks are typically politically or financially motivated. In many cases, the mere threat of a DoS (or DDoS) attack can be enough to extort money from a business, which would lose many times the demanded amount due to interruption.

Threat actors	C2 Servers	Compromised web servers (command re-broadcast)	Compromised web servers (DoS bots)	Targeted victim
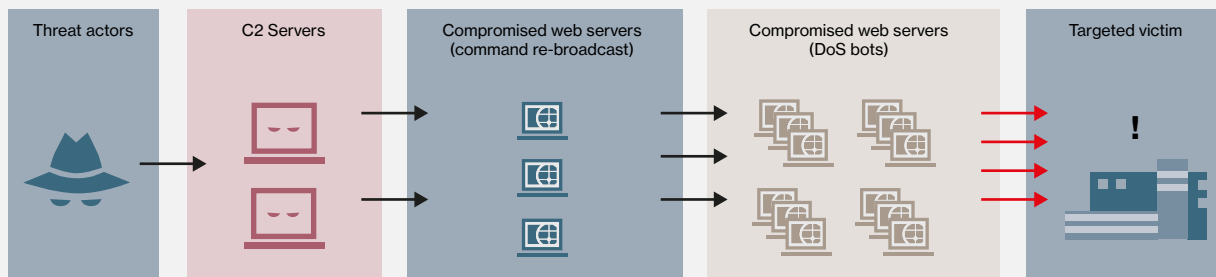
In 2016, a botnet compromising Internet of Things (IoT) devices was used to conduct one of the largest DoS attacks in history. Various devices were infected by a combination of default passwords and an open platform, which was easily hijacked by the Mirai botnet. Despite being defeated by simple controls like using strong passwords on IoT devices or using firewalls to restrict traffic to related subnets, the Mirai botnet was able to grow on the backs of devices likely unknown to, or forgotten by, IT administrators.

DoS attacks can be either large in magnitude or long in duration, but they are typically not both. As IoT devices become more widespread, organizations will need to have increased vigilance over not only inbound flood traffic, but also malicious traffic originating from their own network.

CE-3: ICS Onslaught – the Fiddling Nero

Breach scenario

Breach scenario
Specific

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Crimeware, Insider and privilege misuse, Cyber-espionage, DoS attacks

Time to discovery
H — **D** — W — M — Y

Time to containment
H — **D** — **W** — M — Y

Threat actor

Composition
State-affiliated, Activist, Organized crime

Motives
Grudge, Ideology, Espionage

Tactics and techniques
C2, Scan network, Exploit vulnerability, Disable controls

Targeted victims

Industries
Utilities, Public, Manufacturing, Transportation

Key stakeholders
Incident Commander, Physical Security, Corporate Communications, Legal Counsel

Countermeasures
CSC-1, CSC-2, CSC-3, CSC-8, CSC-19

Description

Industrial Control Systems (ICS) collectively describes various types of systems that manage and monitor industrial operations, such as production. ICS onslaught involves threat actors taking advantage of outdated and un-patched ICS to achieve their goals.
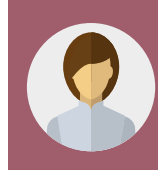
Getting a Grip on Things

Stakeholder

CIP/CS Specialist

The situation

A company, we'll call Gator-Grasp Fasteners, retained the Verizon RISK Team to perform a health check of their industrial environment. This particular customer was in the business of fabricating specialized fasteners, which were required to pass very specific engineering requirements, such as meeting or surpassing certain strength, tensile stress, mechanical properties and material content thresholds.

At the onset of the health check, Gator-Grasp Fasteners' automation engineers expressed skepticism and mild dissent, arguing that a "health check" was not necessary. In their many years of being on the job, the "patient" had always functioned well and had shown no signs of being "unhealthy." So why mess with things? They assured their management that the Operational Technology (OT) environment was secure and that they expected there would be no significant findings. After all, the automation engineers were experts and they knew what they were doing. Nonetheless, management insisted and the automation engineers reluctantly agreed to work with the RISK Team.

> In their many years of being on the job, the "patient" had always functioned well and had shown no signs of being "unhealthy." So why mess with things?

As with any engagement, there was a kick-off meeting, which was used to introduce everyone, set initial expectations, discuss the in-scope environment, request additional information and schedule the onsite visit. The requested information included a list of network segments, IP address ranges, IP address assignments, and an asset inventory.

The Gator-Grasp Fasteners Team was instructed not to create any new documentation in order to avoid a situation where the creation of new documentation would potentially mask a procedural deficiency. In assembling the requested documentation, Gator-Grasp Fasteners quickly realized that what it did have was inadequate.

During the on-site visit, the automation engineers, the RISK Team's Critical Infrastructure Protection/Cyber Security (CIP/CS) specialists and other Subject Matter Experts (SMEs) discussed the various OT systems, in-place security measures and other operational procedures. This included processes and practices (aka "institutional knowledge") that are followed, but were not necessarily documented. These discussions revealed that over the past few months, the network seemed "sluggish," which the automation engineers and SMEs attributed to older, legacy equipment. With an understanding of the situation in mind, we visited various locations where we walked the manufacturing floor and made additional observations.

Compliance is a by-product of security, not the other way around ... or is it?

All too often, the concepts of compliance and security become muddled and muddied. If you speak to 100 different professionals, you will receive 100 different opinions. Herein lays the 101st opinion:

- Compliance and security are distinct disciplines often with shared objectives. It is very easy to be compliant without being secure and it is also possible to be secure (well, relatively speaking – as no environment is ever completely secure) without achieving compliance.

- Compliance requirements set minimum standards, and any organization should endeavor to exceed them with their security controls.

- Security priorities should first be driven by perceived threat analysis and comprehensive risk management, and then be tested for compliance. This should be done rather than using compliance checklists to drive security investment and stopping there.

One of the first things we noticed was some OT systems had anti-virus protection while others didn't. For those that didn't, we were told that, since they were isolated, they didn't need protection. Incredibly, when we looked at the anti-virus logs on the OT systems that had malware protection, we found them replete with malware detections, deletions, and quarantine alerts. Of the 57 systems in total, 33 systems had at least one malware alert, and many had multiple alerts.

When we inquired about these alerts, we found that the automation engineers and operators were well aware. They reasoned that since the malware protection was correcting and "repairing" the problems, everything was acceptable. We explained that there was clearly an underlying problem leading to the repeat infections and recommended a more detailed review to identify the root cause.

Response and investigation

Gator-Grasp Fasteners had no documented IR process for investigating incidents, so we took the lead. The company did not have a centralized logging solution and what devices did log did not provide insight into how the malware was getting into the network. The problem? We needed more visibility.

With the cooperation of Gator-Grasp Fasteners, we set up a Switched Port Analyzer (SPAN) port and deployed a passive network analyzer to collect and analyze the traffic. Using indicators related to the identified malware, we reviewed network traffic and quickly identified multiple potentially infected systems. As we expected, the network traffic revealed malware infections associated with the legacy OT systems that did not have anti-virus protection. Further analysis revealed that a number of misconfigurations existed – which had allowed unauthorized network communication.

The infected systems, many of which were very actively searching for new systems, were a good candidate for the "slow network" problems identified during earlier interviews. Using the collected network traffic, we ran statistics on data transfer rates and quickly realized that the scanning attempts were saturating legacy network connections with probes. With a concrete list of infected systems, we targeted the population of compromised endpoints.

Despite the widespread infection, Gator-Grasp Fasteners had been fortunate. Review of the malware resident on each system revealed common drive-by infections, all targeted at stealing banking credentials. As none of the infected OT systems were utilized for anything other than process management, it was unlikely that further damage had occurred. The network trouble was an unintended side effect of the malware's attempts to find new systems compounded with overly permissive firewall rules.

We provided a list of known infected systems to Gator-Grasp Fasteners, which quickly began rebuilding them from known good images. To keep remediated systems remediated during this process, we continued network traffic monitoring for known indicators and behaviors associated with the identified malware. With the current issue well on the path to being resolved, we turned our attention to the uninfected, but still "troubled" OT systems.

For the customer's ease, we broke down our recommendations into three categories covering their entire OT environment:

1. **Unnecessary legacy systems in unmanned locations.** These systems were removed from the network and decommissioned. These were difficult to track down as they were not documented, making them hard to find, which ultimately delayed the containment and eradication activities.

2. **Necessary legacy systems unable to be protected by an anti-virus solution.** We manually removed the existing malware and the systems were hardened from a best practices standpoint. Stringent firewall rules were deployed to prevent access to and from these systems, which were designed to limit the reach of any future compromises.

3. **New systems not patched or protected by an anti-virus solution.** These computer systems were patched and malware protection was installed.

> I considered documentation a waste of time, but in the end, I realized, there was a lot that I didn't know, and what I didn't know ended up being a big part of the problem.

Lessons learned

Just as in the non-ICS world, a security incident can cause damage to brand reputation, loss of competitive advantage, legal or regulatory non-compliance issues, considerable financial damage, and harm to the environment and community.

The biggest lessons learned could be summed up in one automation engineer's comments: " ... well, being here for over 25 years, I thought I knew all the ins and outs. I didn't consider documentation very important, but in the end, I realized, there was a lot that I didn't know, and what I didn't know ended up being a big part of the problem."

We found there were multiple corrective actions that Gator-Grasp Fasteners needed to take to shore up their detection, mitigation, and response efforts. These were as follows:

- **Perform IR planning.** An IR Plan is critical to resolving security issues by providing direction and guidance to responders.

- **Conduct first responder training.** Train those most likely to identify security issues about the IR Plan; educate them to collect information and triage immediately.

- **Harden OT systems.** Devices with overly permissive default configurations should be reviewed and unneeded configuration options should be disabled, to reduce the risk of misuse.

- **Patch and patch often.** Develop a patch management program to properly secure assets and networks. Security patches fix known vulnerabilities and mitigate the spread of malware.

- **Utilize anti-virus/Intrusion Detection System protection.** Install a host-based anti-virus solution or intrusion detection system on all IT/OT systems and keep the definitions up-to-date.

- **Configure logging, monitoring and alerting.** Centralize logging from all devices into a single location and periodically review logs for signs of suspicious activity such as anti-virus alerts, failed log-in attempts, or network communications involving external systems.

- **Maintain IR/disaster recovery plans.** It is essential to have well-documented and run-tested IR and DR Plans. If not, the response and recovery process will be disorganized, potentially incomplete, and take much longer.
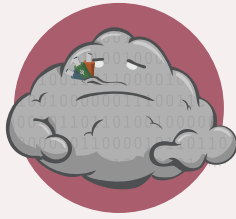
CE-4: Cloud Storming – the Acumulus Datum

Breach scenario

Breach scenario
Specific (Espionage), Indirect (Vulnerability)

Sophistication level
1   2   **3**   **4**   5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Crimeware, Insider and privilege misuse, Cyber-espionage, Web application attacks

Time to discovery
H   D   W   M   Y

Time to containment
H   D   W   M   Y

Threat actor

Composition
Organized crime, State-affiliated

Motives
Financial, Espionage

Tactics and techniques
Export data, Privilege abuse, Capture stored data, Exploit vulnerability

Targeted victims

Industries
Utilities, Public, Manufacturing, Transportation

Key stakeholders
Incident Commander, Corporate Communications

Countermeasures
CSC-5, CSC-6, CSC-10, CSC-14, CSC-16

Description
Security tends to be a challenge when working with data and assets outside of normal environments. Cloud storming attacks take advantage of the proliferation of data stored in the cloud, the inherent shortfalls in outsourced cybersecurity, and the challenge of breach response activities.

When it Pours, it Rains

Stakeholder

IT Security Manager

The situation

Many organizations that are purchasing cloud-based products and "Everything-as-a-Service" offerings have a myopic view when it comes to security. And while it's important to consider the most obvious concern – what if my cloud provider gets compromised? – this is not the only concern. There are also contractual concerns. And concerns regarding sub-contractors. And concerns regarding data geolocation, data privacy, as well as data sovereignty. Many third-party entities typically view any security obligations regarding your data as your responsibility – not theirs – and most legal and regulatory jurisdictions would agree. This became quite clear to me during a recent cybersecurity incident at my organization.

> Many third-party entities typically view any security obligations regarding your data as your responsibility – not theirs – and most legal and regulatory jurisdictions would agree.

It was a late Thursday afternoon, and I was sitting at my laptop with my attention split between replying to a few emails and trying to read one of my favorite InfoSec blogs before heading home for the day. As luck would have it, just as I was putting my laptop into my bag, my desk phone rang. I told myself that it was probably just a vendor trying to sell me something. The phone stopped ringing and the voicemail light remained off – time to head home, or so I thought. No sooner had I slung my bag over my shoulder and started to head out of my office, than my mobile phone started ringing. It was our Chief Security Officer (CSO), John.

After a quick conversation with John, I learned that we had a security incident on our hands involving our e-commerce site. Calls from customers had been coming into our customer service hotline throughout the day – all with the same complaint. Customers would enter their payment details and initially be told that the transaction failed and they needed to try again. Upon trying again, the transaction would complete as normal. While this might happen occasionally, the hotline had received over 100 calls just that day. I was told that the finance team had reached out to our payment processor, who indicated there were no signs of excessive failed transactions and the problem was likely with our e-commerce site.

I decided to do a quick test transaction on our e-commerce site myself in order to see if I could replicate the issue. When the payment page came up for me to enter my credit card details, I immediately noticed something odd: It was missing our standard company headers, footers, and logos, and was simply a barebones payment page. This payment page was not our payment page!

> The finance team had reached out to our payment processor, who indicated there were no signs of excessive failed transactions and the problem was likely with our e-commerce site.

Being the inquisitive person that I am, I entered dummy credit card data and hit submit. Immediately, I received an error page similar to the one our customers described seeing. I was next redirected to try again – this time the payment page looked exactly as it should. My initial suspicion was that someone might have compromised our e-commerce site and added a fake payment page before our legitimate payment page to capture card details. John and I agreed that we needed to activate our Incident Response (IR) Plan and enlist the Verizon RISK Team.

Response and investigation

Our initial conversations with the RISK Team were enlightening. The RISK Team indicated they had seen this same scenario many times before and that it had most commonly been occurring in Europe and Asia. The redirect to our legitimate payment page was the threat actor's attempt to ensure the transaction still completed successfully in an effort to avoid raising customer suspicions.

The challenges with cloud-based investigations

These days, the use of cloud-based services is ubiquitous among both businesses and individuals. Many business applications traditionally managed internally (such as email) are now outsourced to a management company using a hosted solution in the cloud. While the positive impact on service availability and cost reduction are attractive to any organization, there are implications, many of which come to the forefront during a cybersecurity incident response or digital forensic investigation.

Traditional digital forensic tasks — analyzing memory, disk, and network data — are significantly more challenging when physical access to a system isn't possible. Businesses often only realize contractual or technical limitations with accessing "their servers" from a cloud service provider during an incident. Therefore, it's paramount to ensure that your business is ready to respond to an incident. With the additional complexity associated with third-party, managed or cloud services, considering the following questions will help ensure you are as ready as you can be:

- Do we have the tools to capture forensic evidence from remote and outsourced systems?

- Are there limitations as to the level of access we can achieve (i.e., can we only access logical files and as such, have to do without deleted data)? Are we able to get access to our data at all?

- How quickly can we get access to the data? What technical constraints does the remote location impose (e.g., slow transfer speeds)?

- Are service providers contractually obliged to assist during an incident (i.e., have you read the fine print)? If so, what level of service and response are they obliged to provide?

- What type of log data is my service provider retaining and for how long is it retained?

Upfront cost saving is a very attractive prospect; however, the potential cost associated with an incident being impeded by cloud services should not be underestimated. When choosing a service provider, consider their readiness and ability to respond to a cybersecurity incident should one occur.

The RISK Team got right to work and began collecting background details of the incident and an understanding of our environment. They focused in on our e-commerce site, which mostly catered to customers in Western Europe, and was managed by a third-party web developer. The RISK Team joined us on a conference call with our web developer to better understand how they managed our site and plan for how we would collect the necessary supporting forensic evidence.

> The redirect to our legitimate payment page was the threat actor's attempt to ensure the transaction still completed successfully in an effort to avoid raising customer suspicions.

While we knew that the web developer was also in the European Union (Czech Republic), we were not aware that they actually leveraged the services of a low-cost cloud services provider in a completely different part of the world. At this point, the hair on the back of my neck stood up as I could hear the voice of our privacy attorney in my head ask, "Our customer data went (pause) where?"

The RISK Team suggested that we consider taking the site offline to limit any potential for further customer data compromise until the investigation could positively identify the intrusion vector and implement containment and remediation measures. We agreed; and so the web developer immediately disabled the site and replaced it with one of those temporary "Website Undergoing Maintenance" pages. At this point, the clock was ticking as our customers and the public-at-large would eventually realize this was not a normal maintenance window.

We leaned on our third-party web developer to facilitate a conference call with all involved parties, to include the cloud services provider in India. We needed to swiftly gather logs from the segment of the cloud environment that housed our web and database services so we could work with the RISK Team to identify the intrusion vector and at-risk timeframe. During the call, we all learned the cloud services provider in India actually hosted our site together with customer data on systems physically located in a data center in Malaysia. If I hadn't personally been involved with all of these meetings and calls, I would have thought that this was a cruel joke being played by someone.

By the time we engaged our third-party web developer, and they pulled in their cloud provider in India, who then involved their data center manager in Malaysia, two weeks had already come and gone. Thankfully, the site had been offline during this time and so we stemmed the tide of compromised customer data. However, that also meant we were feeling the pain of an e-commerce site that wasn't generating revenue for two weeks and of course a substantial negative impact to our brand image. Fortunately, the RISK Team had local investigative responders and the ability to deploy an on-premise mobile lab, allowing the digital forensics investigation to commence quickly. There were still some hurdles to overcome relating to the cloud provider's multi-tenant environment and the data privacy of their other customers, but the RISK Team made quick work of that based on their previous experience tackling similar challenges.

With the required evidence in hand, the RISK Team was able to quickly confirm initial suspicions. The threat actor had created a fake payment page that was presented to our customers as a means of harvesting their credit card data, after which it would present our legitimate payment page so the transaction could still successfully complete. The digital evidence also revealed the fake payment page was coded to upload in real time the harvested credit card data via Secure Hypertext Transfer Protocol (HTTPS) to an external IP address geolocated in Belarus.

Fortunately, through review of the threat actor's code, the RISK Team was able to determine there was a fundamental flaw in the way it attempted the external connection. This was correlated with the network logs to confirm data exfiltration was never successful. Finally, we got some good news!

Lessons learned

While we faced a challenging situation regarding the compromise of our e-commerce site coupled with exposure risk to sensitive customer data, we also learned a valuable lesson in terms of how critically important it is to know where our data resides. The RISK Team told me they find that all too often organizations struggle to adequately perform asset and data discovery within their own environments, and even fewer organizations have such an understanding when their data extends to third-party entities.

> The digital evidence also revealed the fake payment page was coded to upload in real time the harvested credit card data via HTTPS to an external IP address geolocated in Belarus.

The cascading nature of subcontractor relationships can lead to an organization not fully understanding what legal entities are in possession of their customers' data. This can also be further complicated when those third-parties may have an immature understanding of data privacy, sovereignty protections, and restrictions as they relate to moving such data across specific borders. As evidenced in this particular incident, these types of complications also impact the timeliness of conducting a thorough and proper investigation, as well as the lost revenue associated with the downtime incurred while we unraveled the web of third-party relationships.

In speaking with the RISK Team, I learned another common technical challenge often faced is that many IR Teams and cloud providers often struggle with "carving out" specific customer evidence from multi-tenant cloud-based environments. This can have the adverse impact of preventing a comprehensive root cause analysis, or in some cases, any analysis at all, being carried out. This is the epitome of being kicked while you're already down. Fortunately, the RISK Team was able to assist with the evidence carving, and in doing so, provide a comprehensive root cause analysis. For us, this reinforced the importance of working with our third-party service providers, to ensure they have the architecture to support third-party audits and investigations.

Incident management focus: Data breach notifications

When victim organizations experience a data breach, the usual priority is to contain the incident and restore the environment to normal business operations. However, for breaches involving Personally Identifiable Information (PII) or Protected Health Information (PHI), data breach notifications are just as important. These notifications include required legal and regulatory reporting, employee and customer letters, and media press releases. There are an increasing number of laws, regulations, and industry specific mandates related to breach notifications. The "how" and "when" can vary depending on the jurisdiction, the information involved, and the extent of the breach.

In general, two types of information require breach notifications: (1) various country-specific laws provide for private, governmental, or educational entity PII breach notifications, and (2) the HIPAA Breach Notification Rule and HITECH Act provide for PHI breach notifications.

When designing an IR Plan, the following areas should be covered in terms of data breach notifications:

- **Decision-makers.** Which business units are responsible for the notification process? These typically include Corporate Communications or Public Relations (PR), the Legal Team, and possibly Human Resources (HR). Depending on the size of the data breach a third-party communications firm may also be needed to handle the notification (e.g., send out mailers to breach victims, etc.) and how to engage this firm should be part of the planning process.

- **Notification timing.** There may be an impulse to report findings as soon as these become available; however, it is advisable to use caution and avoid releasing information too quickly. Investigations take time, and it's important to let the process unfold in order to gain an overall picture and the detailed information needed to make an informed notification. This helps reduce the need for follow-up releases to correct the information, which add confusion to the situation.

- **Incident responders.** For incident responders, specific requests for information may come from many sources. These requests may include, but not necessarily be limited to, the following:

  - summary/nature of incident/breach timeframe

  - names (and overall number) of impacted customers/employees

  - incident containment status

  - any changes to business processes

The notification process is an important component of handling data breaches. In addition to technical abilities to remediate the compromise, a thorough understanding of state, federal, and industry notification laws and regulations is also essential. Being in tune with these compliance requirements and taking a proactive approach to identify the procedures required to meet them can make all the difference when dealing with a live incident.

Malicious software

Malicious software (malware) is a favorite tool of threat actors. Malware comes in all shapes and sizes, but perhaps can best be characterized by what it is intended to do. It is designed to take over, damage, and/or exfiltrate data from a system, as well as attack other systems, and/or gain additional insight into a system or its network.

The most common forms of malware include Trojans, viruses, worms, backdoors, Command and Control (C2), spyware, keyloggers, sniffers, password dumpers, RAM scrapers, rootkits, data exporters and adware, among others.

The three primary purposes of malware are to establish a beachhead, collect data, and exfiltrate data. This is reflected in the Top 5 malware varieties that we've seen within the VERIS data over the previous three years for data breaches only:

Ranking	Asset	Frequency
1.	Export data	55.6%
2.	C2	49.2%
3.	RAM scraper	44.8%
4.	Spyware/Keylogger	42.9%
5.	Backdoor	23.1%

Scenario MS-1 (Crypto Malware) covers a ransomware incident that encrypted critical files necessary for the victim organization's business operations. Scenario MS-2 (Sophisticated Malware) changes things up a bit and discusses complex malware and the challenges faced in investigating these attacks, and Scenario MS-3 (RAM Scraping) deals with the challenges faced with Payment Card Industry (PCI) forensic investigations and RAM-scraping malware. Scenario MS-4 (Unknown Unknowns) describes a malware outbreak and leveraging endpoint detection and response capabilities (EDR) to identify and respond to the issue at hand.

Malware spotlight: Exploit kits

Exploit Kits, or EKs, are frameworks used for attacks against web browsers, which rely on malicious software hosted on a web server and are designed to spread malware. These kits identify and exploit security flaws found in client machines by taking advantage of vulnerabilities in browsers or their many plugins. Most browsers run with multiple plugins enabled, many of which may not be updated. Due to this, exploit kits are able to compromise machines without the use of a zero-day vulnerability. This has made EKs very effective and widespread, something that can be seen in their persistence.

The first known EKs date back to 2006, and since then, have been used to distribute a wide variety of malware. To avoid detection and exploit new vulnerabilities, EKs constantly change, leading to multiple variants based on the same core kits. These adaptations each focus on the specific needs of a threat actor or campaign. New EKs with additional features frequently replace or shut down outdated versions. For example, in June 2016, after a successful two-year run, Nuclear EK was dismantled and stopped serving malware. Shortly afterwards the Neutrino EK rose to lead the pack, distributing massive amounts of the Cerber ransomware.

In recent months, the RIG EK and its variants have emerged as the leading EK, being heavily used in malvertising such as EITest, pseudo-Darkleech, and Afraidgate campaigns. The payloads usually target banking information or deliver ransomware, which the threat actors control. The flexibility of RIG EK is apparent in the variety of malware it distributes, ranging from botnets like Tofsee, Gootkit, and Vawtrak to ransomware like Locky and Cerber. Multiple variants of the RIG EK have been found in the wild, each adapted to a specific need. The RIG-v variant uses a modified encoding and landing page Uniform Resource Identifier (URI) to avoid detection by existing signatures. The RIG-e, or Empire Pack, included an updated interface to make managing multiple campaigns easier for threat actors. RIG-e was notably recently used as part of the EITest campaign.

MS-1: Crypto Malware – the Fetid Cheez

Breach scenario

Breach scenario
Opportunistic

Sophistication level
1 — 2 — 3 — 4 — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Crimeware

Time to discovery
H — D — W — M — Y

Time to containment
H — D — W — M — Y

Threat actor

Composition
Organized crime

Motives
Financial, Grudge

Tactics and techniques
Phishing, Ransomware, C2, Exploit vulnerability

Targeted victims

Industries
Varies (Opportunistic)

Key stakeholders
Incident Commander, Legal Counsel, Corporate Communications

Countermeasures
CSC-5, CSC-6, CSC-7, CSC-10, CSC-13

Description

Crypto malware, a form of ransomware, is malware that prevents users from accessing their system, file shares or files by encrypting the data. After gaining access and control, threat actors hold the data for "ransom" until the user agrees to pay for regaining access to their data.

Back up to Normal

Stakeholder

CISO

The situation

With a few months under my belt as the Chief Information Security Officer (CISO), I was starting to learn the inner workings of my new employer. Things had been going smoothly with no major incidents until late one afternoon when the Security Operations Center (SOC) Manager came to my office. Key business-critical applications were offline and impacting daily operations for the organization including customer-facing areas. The IT Operations Team had done an initial review. This review found multiple servers with filenames and extensions changed on network shares, as well as ransom notes residing in directories.

> This review found multiple servers with filenames and extensions changed on network shares, as well as ransom notes residing in directories.

Response and investigation

This was a classic example of a ransomware infection and something we knew was a very real threat. I had discussions with my team and colleagues about putting together a playbook for this same scenario and we were even planning to use such a scenario in next quarter's tabletop exercise. My team had a skeleton of a plan to respond to a ransomware attack, but we had not fully flushed out the details and socialized it with the rest of the organization.

> Within minutes, the SOC, the IR Team, and other stakeholders for the impacted business units had assembled in the "SOC War Room," either in person or via our conference bridge.

Within minutes, the SOC, the Incident Response (IR) Team, and other stakeholders for the impacted business units had assembled in the "SOC War Room," either in person or via our conference bridge.

Per our IR Plan, my deputy CISO took on the responsibilities of Incident Commander and led the technical aspects of the response. Meanwhile, I prepared to coordinate with the Executive Committee and Crisis Management Team, who were anxiously waiting for updates on our response strategy, progress, the business impact and, just as importantly, when the business would get back to normal.

> With the impact to the business being critical, there was pressure to perform the remediation efforts in parallel with the investigation.

With the impact to the business being critical, there was pressure to perform the remediation efforts in parallel with the investigation. The compromise was to begin review of the backups from the impacted systems to determine the availability of the data and the time needed to restore normal business operations.

While these efforts were underway, I directed the IR Team — which was working with the Verizon RISK Team — to continue with their investigation of the incident. As part of their initial findings, the modified files on the network shares were all shown to have been last modified by a network administrator's account, which also had domain admin rights. I directed them to disable the account for that user, begin collecting logs related to the user's activity, and to collect the administrator's laptop for forensic analysis.

Next, it was back to the issue of how to restore the systems to a prior working point. The update from the Business Continuity Team was varied based on the application or systems in question. For some, the solution was a quick fix of just restoring the individual files from the most recent backups in order to return to normal business. As for others, some systems hadn't been included as part of the backup routine so those files needed to be located from other sources ranging from local copies saved by users, to the reinstallation of applications. Virtual machines were quickly fixed by restoring from a recent snapshot. The worst-case systems, which fortunately for us were limited in number, could not be recovered.

By this time, initial findings from analysis and talking to the user in question revealed that the network administrator had opened an email attachment. This attachment had contained one of the latest ransomware variants that exploited an application vulnerability. Unfortunately, for us, this vulnerability hadn't been patched in our environment.

While most of the data was restored, there were still files that were not recoverable. It was at this point the Executive Committee began considering paying the ransom in order to get the data back. This was seen as the lower cost option; however, there was concern as to whether we would actually get the files back. Would we be supporting the threat actors by acting as a weak target and possibly inviting a repeat of this attack but at a larger cost? The final decision was made not to pay the ransom, as this would have supported the people behind the ransomware.

> Within a week, I presented these recommendations to the Board of Directors, which had gathered specifically to be briefed on the details and outcome of this incident.

Lessons learned

Upon conclusion of the incident, I directed a "lessons learned" effort by collecting feedback from each individual involved in the response to this incident. Upon reviewing all of the input, my team and I compiled a list of recommendations the company should implement. The recommendations were designed to reduce the likelihood of this happening again as well as identify response processes to improve or change in the event of a reoccurrence.

These represented items that could be implemented immediately along with items for which longer-term plans and changes to corporate policy would be necessary. I presented these recommendations to the Executive Committee and, upon receiving their concurrence, we set about implementing them throughout the company. Within a week, I presented these recommendations to the Board of Directors, which had gathered specifically to be briefed on the details and outcome of this incident. Some of the recommendations presented were as follows:[8]

Mitigation

- Patch third-party applications as soon as possible.

- Test and validate data backup processes.

- Deploy Group Policy Objects (GPOs) to block executable files and disable macros.

- Block certain email attachments.

- Remove local administrative rights.

Detection and Response

- Deploy a File Integrity Monitoring (FIM) solution.

- Educate and sensitize users.

- Update host-based and enterprise anti-virus solutions.

- Block access to Command and Control (C2) servers.

- Set file shares to read-only mode.

- Check encrypted file ownership to determine infected users.

- Recall known phishing emails from user mailboxes.

- Take infected systems offline.

8. In November 2016, the Verizon RISK Team published an update to Scenario #15 of the 2016 Data Breach Digest, "Data Ransomware – the Catch 22" entitled "Data Breach Digest – Update November 2016, Data Ransomware: User and File Space Error." This update offered several mitigation and response recommendations. Further details for the recommendations below can be found in this update.

Incident management focus:
Digital evidence handling

Before, during, and after a cybersecurity incident an organization's technology environment should be treated like a "crime scene." This means that digital evidence should be collected and preserved in a manner consistent with best practices. Digital evidence may be composed of volatile data, memory dumps, forensic images, logs or any other data element that could help prove that a cybercrime was committed. As a result, first responders should adhere to two key digital evidence-handling guidelines:

Preservation – It is extremely important that first responders properly preserve digital evidence by using forensically sound collection practices. This can be accomplished with the use of forensic acquisition tools and techniques that prevent or significantly reduce changes to original digital evidence sources. If collecting data from a live system, first responders should use a repeatable process that minimizes their interaction with the system. The less interaction an individual has with a system the better.

Integrity – Once digital evidence preservation has occurred, the next step in digital evidence handling is to maintain the integrity of evidence collected. This can be accomplished by first computing and documenting the hash value (MD5, SHA1, SHA256, etc.) of the digital evidence source. This allows additional parties to re-compute the hash value later on to ensure that nothing has changed from the original digital evidence source.

Finally, it is also important to maintain the appropriate chain-of-custody for evidence transferred between parties. The chain-of-custody form documents who has had access to evidence, when they had access and why the evidence was transferred.

MS-2: Sophisticated Malware – the Pit Viper

🛡 Breach scenario

Breach scenario
Specific

Sophistication level
1 — 2 — 3 — **4** — 5

Attributes
Confidentiality, Integrity

🕐 Incident pattern

Pattern
Cyber-espionage, Crimeware, Insider and privilege misuse

Time to discovery
H — D — **W** — M — Y

Time to containment
H — **D** — W — M — Y

⚠ Threat actor

Composition
State-affiliated, Organized crime

Motives
Espionage, Financial

Tactics and techniques
Use of backdoor or C2, C2, Spyware/Keylogger, Backdoor, Downloader, Capture stored data, Scan network, Password dumper, Exploit vulnerability, Rootkit

◎ Targeted victims

Industries
Public, Manufacturing, Transportation, Information

Key stakeholders
Incident Commander, Legal Counsel, Corporate Communications

Countermeasures
CSC-6, CSC-8, CSC-12, CSC-13, CSC-16

Description
With the efforts made to enhance security through segregation and defense-in-depth principles, threat actor activities have become increasingly complex. Enter sophisticated malware. In some operations, threat actors increase their sophistication through malware to achieve their goals.

The Distinguished Gentleman from Saskatchewan

Stakeholder

Malware Reverse Engineer

The situation

When compromising secure environments that utilize proper segregation and security controls, threat actors must leverage methodologies that are more complex. These tactics often involve highly sophisticated malware with unique capabilities. Over the course of a breach, threat actors first secure exfiltration points on the perimeter with beaconing or listening malware. Such exit points are meant to be redundant for better resilience. Pivot systems are then infected with additional malware in an effort to trace a path to the target. Finally, once the target is infected, the threat actors can begin the process of moving data out of the environment.

In my experience as a Malware Reverse Engineer on the Verizon RISK Team, I have seen the first sign that something is wrong often comes with the discovery of an infected system. Whether this system was discovered via common point of purchase analysis or recurrent server crashes, the problem remains the same. In both cases, the detection does not come from security controls, but rather from direct impact after the fact. This aspect and characteristic of sophisticated malware was highlighted in last year's Data Breach Digest, "Scenario #16: Sophisticated Malware – the Flea Flicker."

> These sophisticated attacks evade security controls, making detection difficult. They often result in business-critical functions being disrupted long after the first system was infected.

These sophisticated attacks evade security controls, making detection difficult. They often result in business-critical functions being disrupted long after the first system was infected. A module designed to sniff the network or the index mailbox information is much more likely to crash than a simple command and control client module. When systems, such as the mail server or a required application, crash, they generally get more attention than an employee's workstation that is just "running slowly."

These targeted systems, while being the source of exfiltrated data, frequently do not interact with obvious malicious endpoints because they are just collection nodes. Trying to identify a root cause with only a collection node to review can be very frustrating because collection nodes often do not contain actionable network Indicators of Compromise (IoCs) that would enable enterprise-wide detection or containment. Instead, these nodes relay valuable information to other internal systems, which in turn relay that data externally.

With so many legitimate internal connections, identifying unauthorized communications can be a difficult and time-consuming process. Even when samples of the malware are captured, behavioral analysis of such malware is usually inconclusive or incomplete due to the decentralized nature of the architecture. To proceed to the next step you need to understand the malware internals. You need to understand how nodes communicate and how data is stored internally. Answering these questions usually requires escalation to a reverse engineer.

Response and investigation

We reverse a wide variety of malware collected from different types of incidents around the world. More sophisticated malware is often highly customizable, leveraging a common core (the "brain") and an extensive set of modules. The core of this malware ensures that it persists on the device in addition to managing dynamic loading of these modules as needed. Depending on the overall purpose of the malware, we may see modules designed for exfiltrating data on common protocols like Hypertext Transfer Protocol (HTTP) or Domain Name System (DNS), conducting reconnaissance, or searching for credit card track data.

Due to the highly modular nature of these types of threats, an infected system can be used in many different ways and reconfigured on the fly—allowing threat actors to maintain access even when certain systems are remediated.

In some cases, this type of review is particularly challenging because malware is only resident in memory on infected systems. While functions related to persistence may exist on the disk, modules related to covert activity or encryption methods are stored only in memory. Conducting analysis on these aspects of malware required the creation of specialized tools and methods to pair with traditional disk forensics.

Regardless of the incident scenario, one of the first tasks when reviewing infected systems is to create a network map of systems and functions based on available data.

Reverse-engineered modules and data extracted from files are categorized by system to produce a high-level view of the infection. The results of this analysis can be combined with network information, such as full packet capture or NetFlow, to further identify discrete communications and timelines of activity.

This "network within the network" can be used to determine how a threat actor gained access and to help scope additional systems to review or remediate. A complete map enables us to detect the entire infection before proceeding with containment. Unfortunately, in most cases the pressure for rapid containment outweighs the desire to wait for this infection map to be complete.

Any premature remediation can have a serious effect on our ability to conduct a thorough review; we frequently have to fill in the gaps using prior knowledge. Anti-virus, while definitely an essential part of good security posture, is a double-edged sword as it often reduces the number of viable samples for us to review. Automatically quarantined or purged files may be lost forever and leave missing pieces in the puzzle.

When dealing with memory-resident malware, simply powering down or rebooting the system can erase evidence of the infection forcing analysis to rely on lower-fidelity logs or network data.

Threat actor tool: PowerShell

PowerShell is a very powerful scripting language built into Windows for system administration and the automation of various tasks. Microsoft has even gone so far as to open source the framework and release packages that can be installed on Linux and Mac. This has allowed PowerShell to grow into a well-supported and well-used platform across major operating systems in data centers around the world.

Both IT administrators and threat actors often use PowerShell, and many of the same commands. The heavy usage of PowerShell can cause a lot of headaches in cybersecurity incident scenarios, as it can be difficult to determine authorized usage by threat actors from legitimate use by system administrators. As such, it is very important to have a tight hold on which systems can utilize this powerful framework.

Some tips for securing systems with PowerShell installed are:

- Configure the PowerShell Execution Policy relative to the server's purpose. Production systems should be set to "AllSigned" if script execution is required, and "Restricted" if not. Development systems should never be set lower than "RemoteSigned." Avoid "Unrestricted" Execution Policies as they allow remotely downloaded systems to run by default.

- Keep an inventory of PowerShell-enabled systems and ensure proper logging and retention is in place to provide data to responders in the event of an incident.

- Be aware that most default PowerShell configuration options represent the highest level of security. Changes to these options should be carefully considered and an audit log of when and why options were changed should be kept.

When conducting a review without all of the details, we frequently see containment and mitigation efforts take longer than expected. Without the full context of the malware's capabilities and communication methods, infected systems can stay hidden for a long time, especially if the threat actor is aware of the remediation efforts and purposely attempts to preserve access. In addition to existing logs, greater network visibility is often required to help track down unknown infections based on information collected from known infected systems. If it does not already exist, adding this visibility can lengthen the remediation phase allowing the threat actors opportunity to react. Infected systems missed during a remediation phase will show up again later, and we frequently see repeat incidents due to incomplete eradications.

Lessons learned

It may not always be possible to postpone remediation activities until a full review of sophisticated malware can be completed, but some triage needs to be done before actions are taken. Early actions can wipe out artifacts and leave responders with one hand tied behind their backs. A balance between understanding the infection and responding to the threat must be maintained for long-term success.

Mitigation

- Centralize and monitor log sources for unauthorized or suspicious activity.

- Segment important systems and limit the allowed network connections to reduce potential paths.

- Implement ingress/egress monitoring for unknown communications.

- Educate first responders on the importance of and process for evidence collection.

- Run up-to-date anti-virus software to limit the capabilities of threat actors.

Response

- Remove infected systems from the network, but leave them powered on.

- Draw a network map of infection; use it to drive the investigation.

- Declare containment only when all outbound traffic vectors are identified.

- Preserve all artifacts before eradication.

- Gather and retain information about the infection.

Incident management focus: Digital forensics firm on retainer

You know the threat landscape and understand the risks they pose to your organization. You know it's not a matter of "if" but rather "when" a cybersecurity incident will occur; however, awareness does not always equal readiness. Are you prepared to respond when a cybersecurity emergency arises? Do you have the expertise and resources or, perhaps just as importantly, can you quickly engage the help you need, when you need it the most?

If your answer to those final questions involves anything other than a confident and emphatic "yes," then you should consider a third-party firm on retainer that has emergency response as its heart and soul. The benefits of having an investigative response firm on retainer include:

- Get help when you need it from a trusted partner with whom you are already familiar.

- Avoid having to "shop around" and negotiate a contract during times of crisis.

- Engage experienced, knowledgeable experts in digital forensics, incident response, malware analysis, cyber intelligence and other security services.

- Improve and mature your response capabilities with document review, response training and tabletop testing.

Think forward. Be proactive. Be prepared.

MS-3: RAM Scraping – the Bare Claw

Breach scenario

Breach scenario
Indirect (Vulnerability)

Sophistication level
1 — **2** — **3** — 4 — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
POS intrusions, Insider and privilege misuse

Time to discovery
H — **D** — W — M — Y

Time to containment
H — **D** — W — M — Y

Threat actor

Composition
Organized crime

Motives
Financial

Tactics and techniques
Export data, RAM scraper, Spyware/Keylogger, Capture stored data, Exploit vulnerability

Targeted victims

Industries
Retail, Accommodation, Healthcare, Administrative

Key stakeholders
Incident Commander, Corporate Communications

Countermeasures
CSC-2, CSC-7, CSC-8, CSC-13, CSC-19

Description
RAM scraping is an evolution of traditional data theft tools designed to bypass on-disk or network-based encryption. By accessing credit card information immediately after a card swipe, while it is still in memory, a RAM scraper is able to collect the data in plain text, prior to any encryption.
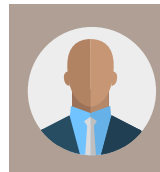
Dealing with Memory Loss

Stakeholder

PFI Investigator

The situation

Organizations with robust security postures still contain desired data, which drives threat actors to find new methods of access. Solutions that encrypt data at-rest on the file system or in-transit over the network have reduced the locations of credit card data – thus threat actors have moved closer to the source.

> Solutions that encrypt data at-rest on the file system or in-transit over the network have reduced the locations of credit card data – thus threat actors have moved closer to the source.

This was definitely the wrong day to oversleep, I thought to myself as I rushed into the office. I was already 20 minutes late for an emergency meeting between my boss and some Verizon RISK Team investigators. We had just been notified of a breach involving our credit card processing systems and were now heading into a Payment Card Industry Forensic Investigation (PFI). This PFI would focus on determining the extent of the incident and identify whom, if anyone, needed to be notified about the issue. I quietly snuck into the back of the conference room, pulled out my notebook and tried to catch up.

Response and investigation

IT Security Manager: We've been using end-to-end encryption in our environment for years so there's no way the threat actors could be pulling any payment card data off the wire. Do you have reason to believe otherwise?

RISK Team PFI: Well, prior to 2009, most payment card data was stolen off the wire using network packet sniffers. This was possible because most organizations were sending unencrypted card data through their internal networks; they only encrypted before sending to their payment processor. Threat actors were able to intercept payment card data during these transmissions and siphon it off. In response to these packet-sniffing attacks, many organizations began using end-to-end encryption solutions like yours. These solutions encrypt data in transit, rather than only when it sits on the disk.

Unfortunately, even with this end-to-end encryption, there still exists a weakness in the crucial moments between when a payment card is swiped and when it is actually encrypted. For a short time, the data resides in memory in an unencrypted format before the encryption operation is completed. Around 2009, threat actors began to adapt their tactics to scrape payment card data directly from a system's RAM, or memory, prior to encryption rather than sniffing it while moving across the network.

Incident pattern: POS intrusions

A Point of Sale (POS) intrusion is a remote attack against network resources where payment transactions are conducted. Most attacks follow the general pattern of: compromise the POS device, install malware to collect magnetic stripe data in process, and retrieve data. Threat actors can then sell the data to criminals who specialize in encoding the stolen data onto any card with a magnetic stripe, and use the cards to buy gift cards and high-priced goods. The trend of adding POS memory-scraping modules to existing malware families continued into 2016. Examples of malware targeting POS systems from this past year are ModPOS and Kasidet Distributed Denial of Service (DDoS) malware.

There are hundreds of sites online selling stolen account data, but Joker's Stash and Rescator are two of the most prominent illicit carding forums. They served as the distribution point for some of the most well-known breaches over the past two years in the hotel, restaurant, and retail industries.

IT Security Manager: So the payment card data is captured by malware between swipe and encryption? Is this attack limited to only swipe transactions where a card is physically present or can it be used against e-commerce? We do have a large e-commerce business.

RISK Team PFI: No, it is definitely not limited to swipe-based transactions. E-commerce-based transactions can suffer from the same vulnerability, albeit in a slightly different way. When a web page captures a customer's payment card data in a web form, that data also exists in memory for at least a short period of time prior to being encrypted and transmitted. The RAM-scraping malware on an e-commerce system or even a customer's personal computer could intercept payment card data similar to a terminal or card swipe device.

> When a web page captures a customer's payment card data in a web form, that data also exists in memory for at least a short period of time prior to being encrypted and transmitted.

IT Security Manager: This sounds like a really difficult problem to solve. Are third-party notifications common in these sorts of events?

RISK Team PFI: Yes. A large majority of these investigations begin with a third-party notification from a law enforcement agency or one of the credit card brands. Off the top of my head, I can only think of one PFI at a major retailer that we worked on that wasn't the result of a third-party notification. That was a unique circumstance where the entity self-identified the incident because the retailer's systems were so archaic, that the RAM scraping being performed by the threat actors was impacting system performance. Employees were complaining of very slow or unresponsive systems.

> A large majority of these investigations begin with a third-party notification from a law enforcement agency or one of the credit card brands.

A small investigation performed by their internal team uncovered malware on the PCI terminals. Just to be clear, this anecdote is not meant to imply that running old hardware on PCI terminals is an effective solution for protecting against or identifying RAM-scraping-based attacks. Sorry, we always have to include that disclaimer with that story.

IT Security Manager: What type of evidence will you usually find in an investigation like this?

RISK Team PFI: That's a difficult question to answer completely, but here's what we normally see. After compromising the external network, gaining the proper privileges and performing reconnaissance to find systems that transact payment card data, the threat actor usually deploys a two-step process.

First, we typically find that the threat actors will start by downloading additional tools that they need to identify where the payment data is stored. We refer to this as "Phase 1" and the types of tools downloaded usually consist of very simple memory tools. These tools are designed to dump or parse the memory of each individual process running on a system looking for payment card data. These tools do not normally have any built-in persistence and are typically used once during the setup phase. Tools such as these have a very low likelihood of being identified by anti-virus software because in many cases they are simply legitimate administrative tools being used for nefarious purposes.

> After having identified a process that contains payment card data, the threat actor will then deploy the actual RAM-scraping malware.

After having identified a process that contains payment card data, the threat actor will then deploy the actual RAM-scraping malware. This "Phase 2" malware will typically have a persistence mechanism, usually in the form of a Windows service, and will dump harvested payment card data onto the system disk in an encoded format.

IT Security Manager: Why would they dump the data in an encoded format?

RISK Team PFI: That's their method of circumventing any potential Data Loss Prevention (DLP) solutions that could identify plain-text payment card data on disk. Sometimes exfiltration will be part of the automated process, but not always. In most of our investigations, these also have a low likelihood of being identified by anti-virus or DLP software due to this obfuscation and other anti-detection techniques. Even unsophisticated threat actors will first test their malware against anti-virus scanners to ensure they're not flagged inside an organization's environment.

IT Security Manager: So if I can't trust anti-virus to protect my organization from RAM-scraping malware, what steps can I take to mitigate the risk?

> A properly configured FIM tool can alert incident responders and security personnel to the introduction of files to a system handling sensitive information.

RISK Team PFI: It's important to remember that RAM scraping is a post-compromise event and there should be many security hurdles between an external threat actor and a payment card data environment. Keeping them out in the first place is the best line of defense against these types of attacks; however, if we're just limited to the realm of mitigating RAM scraping, there are a few steps that can be taken. In contrast to end-to-end encryption, point-to-point (PtP or P2PE) encryption encrypts PCI data at the time of swipe and is a very strong defense against RAM scraping.

Another option to protect POS terminals is File Integrity Monitoring (FIM). Regardless of the type of malware deployed, the initial phase typically involves downloading the tools required to set up the RAM scraper. In most cases, the threat actors will have to introduce files to the system disk to do so. A properly configured FIM tool can alert incident responders and security personnel to the introduction of files to a system handling sensitive information. There are also other options like application whitelisting, which restricts the execution of unapproved binaries. Restricting permissions and not having users accessing the devices with local administrative rights could also help limit the spread of malicious software.

It is also important to remember that proper security hygiene is achieved through a layered approach. The payment card environment should be thoroughly protected through network and system-based security controls on the corporate network. Once a threat actor has introduced a RAM scraper onto a system transacting PCI data, you've already failed the test.

Lessons learned

I left the meeting with my head spinning and a few pages of notes. I looked over our options for these "RAM scrapers." Mitigation included implementing P2PE encryption, using FIM, whitelisting applications, restricting applications from running in temporary file system locations, and using multi-factor authentication. In terms of response activities, engaging a digital forensics firm immediately upon identification of a compromise and remembering not to power-down affected systems; I may need the volatile data in physical memory!

Uh-oh! My acquirer told me I have to undergo a PFI investigation — what's a PFI?

If you have been required by any of the Participating Card Brands (Visa, MasterCard, American Express, Discover, and JCB) to undergo a Payment Card Industry Forensic Investigation (PFI), a forensic investigation of a security issue, it is beneficial to understand the roles and responsibilities of the various stakeholders involved in a PFI investigation.

First and foremost is the merchant that is suspected of having incurred a security breach that potentially exposed payment card data to compromise. In this scenario, the Payment Card Industry Security Standards Council (PCI SSC) defines the suspected compromised merchant as the "Entity Under Investigation." The Entity Under Investigation is required to comply with the Payment Card Brands' operating rules, engage the services of a PFI to conduct the required PFI investigation, and cooperate with the PFI, the Acquiring Bank and the Participating Card Brands during the PFI investigation.

The PCI SSC is responsible for managing the PFI Program, including qualifying the PFI entities that participate in the program, as well as providing training on the PCI standards and PCI SSC programs. The PCI SSC is not involved in the actual conduct of the PFI investigation or the review of PFI reports.

Each Participating Card Brand is responsible for developing and enforcing its own programs regarding when and how PFI investigations may be required and the imposition of any fines and/or penalties related to cardholder data compromise.

The Acquirer, also known as the Acquiring Bank, is a financial institution that enters into agreements with merchants to accept the Payment Card Brands' branded cards as payment for goods and services.

PFIs have been approved by the PCI SSC to perform PFI investigations in the specific PFI regions for which they have been qualified by the PCI SSC. In considering a PFI, in addition to being approved by the PCI SSC, other considerations are:

- How long has the PFI been conducting PFI investigations?

- How will the PFI work with my company during the investigation? Are they solely beholden to the PCI SSC? Will they share results with me? Will they share details that may be helpful to me in protecting my company and my customer's data?

- Has the PFI ever been delisted from the authorized PFI list? Is there any other derogatory information regarding the PFI and their PFI status?

MS-4: Unknown Unknowns – the Polar Vortex

Breach scenario

Breach scenario
Specific, Indirect, Opportunistic

Sophistication level
1 — 2 — 3 — 4 — 5

Attributes
Confidentiality, Integrity

Incident pattern

Pattern
Cyberespionage, Crimeware, Insider and privilege misuse

Time to discovery
H — D — W — M — Y

Time to containment
H — D — W — M — Y

Threat actor

Composition
State-affiliated, Organized crime

Motives
Espionage, Financial

Tactics and techniques
Use of stolen credentials, Use of backdoor or C2, C2, Backdoor, Downloader, Scan network, Password dumper, Exploit vulnerability, Rootkit

Targeted victims

Industries
Manufacturing, Transportation, Public, Healthcare

Key stakeholders
Incident Commander, Legal Counsel, Corporate Communications

Countermeasures
CSC-6, CSC-8, CSC-12, CSC-13, CSC-16

Description
Knowing what you don't know is a far better situation than not knowing what you don't know. Unknown systems, accounts, software and data act as landmines for enterprises. Hidden and ready to detonate, these "unknown unknowns" can explode any time, resulting in substantial impact to operations or public perception.

Sifting Through the Detritus

Stakeholder

EDR Technician

The situation

Even if it's anecdotal, it seems that incidents always happen late in the afternoon. This particular afternoon, I was sitting in on a service review meeting with the Verizon RISK Team and Bill, the IT Security Team Lead, for one of our gaming customers. In addition to the regular discussion points, I was there to explain our Endpoint Detection and Response (EDR) capabilities, and in particular, how we used these for incident response. Halfway through my opening slide, Bill's smartphone rang and upon answering it, his face turned sour. He mentioned he was on-site with our team and the next thing we knew his Chief Information Security Officer (CISO) was on speakerphone and we were scoping an incident.

The CISO, Jack, quickly explained that they suspected their production network had been hacked and that gamer points were being siphoned off from top accounts. The nature of the incident had Jack very concerned that customers' personal information might be exposed as well. Initial reports showed unauthorized access to various systems from a domain admin who was known to be on vacation that week. With the situation still evolving, we knew it merited an immediate response, and so we quickly repacked our bags and hopped in Bill's car for a ride to his office.

Incident pattern: Crimeware

Crimeware-as-a-Service (CaaS) providers offer hacking services that allow individuals to gain access to computer systems or networks at a reasonable price. CaaS has allowed less technically sophisticated individuals to utilize crimeware for their own illicit activities. Typically these individuals are motivated by financial gain or the need for sensitive information and employ threat actors to use weaponized documents, website drive-by downloads and phishing to install malware and compromise systems.

The majority of these services are Remote Access Trojans (RATs) used for spying purposes. For instance, the GovRAT 2.0 can be used to spy on government agencies for as little as $1,000. On the other hand, the popular cross-platform Adwind RAT can be used to spy on individuals for as little as $40. Other CaaS includes intelligence gathering, backdoors, exfiltration, keyloggers or spyware, ransomware, botnets, DDoS attacks and device tracking.

The evolution of CaaS follows similar patterns seen in a business market model used by Software-as-a-Service (SaaS). The model for CaaS has three major components, all operating in the darknet: the developer, the back office support and the cybercriminal. The developers are the brains behind the operation; they are creators of malicious code. The back office support is made up of marketing folks, training support and resource-based providers — such as a bulletproof hosting service. Lastly, the cybercriminal is the individual or group interested in purchasing the malware. The CaaS model has become a major part of the growth of the dark web ecosystem.

Response and investigation

While we drove to the office, Jack's team had been collecting network and application logs from their event management system. These logs had been uploaded to a RISK Team secure file server and by the time we arrived onsite, preliminary intelligence results were in my inbox. It was now late and the fact that both the Chief Information Officer (CIO) and CISO were still onsite and with their sleeves rolled up captured the true gravity of the situation. Beyond the panic of the data loss, the customer had a new release planned for early the next month – something they could not do if their network was crippled.

While my boss worked with the CISO to create a high-level remediation plan, I went to work trying to track down the problem. The intelligence report sent to me contained a number of network-based indicators, which all pointed to a Poison Ivy infection. I knew systems infected with a remote administration tool such as this were likely to be multi-purposed and would invariably only represent one of the pieces of malware discovered. Firewall logs related to these suspect systems revealed widespread scanning on both Remote Desktop Protocol (RDP) and NetBIOS protocols as the infected system attempted to compromise other systems. The list of potentially-affected systems grew with every scan and it was up to me to find a way to triage the larger list.

> Beyond the panic of the data loss, the customer had a new release planned for early the next month – something they could not do if their network was crippled.

The first step involved collecting a sampling of forensic images of potentially infected systems and validating the compromise. The images themselves took a few hours to collect, but review quickly revealed additional artifacts, which pointed us to the location of the malware as well as its output files. These file-based indicators definitely piqued my interest as it meant an EDR solution – exactly what we were trying to demonstrate the value of prior to the incident – was the perfect solution. We were lucky that so far all systems identified as infected were part of the customer's primary domain. This domain supported remote software installation via an automated process, which meant we could quickly push out endpoint agents to all potentially affected systems.

With endpoint detection capabilities in place, I was able to correlate the suspect systems, based on network traffic, with known system-based artifacts. The combination allowed me to reduce the total list of infected systems down to only 15, which then needed further review. These systems were then collected and reviewed to identify additional malware variants.

> It was further determined that the employee assigned to that user account had long since left the company and was not available for comment.

Of the 15 systems, 14 were known either as workstations or as back-end resources used to process game point transactions. The anomalous 15th system presented a new question beyond why it was infected. We needed to know what it was doing on the network in the first place. The customer collected domain authentication logs and found there had only been one user account that had connected to the device, but there had been no connections to the device in over a year. It was further determined that the employee assigned to that user account had long since left the company and was not available for comment.

With the help of the CISO, we were able to identify this former employee's manager, who luckily still worked for the company. After a few minutes of discussion and reviewing the unknown system it was determined the system was a relic of a previous proof of concept. The server was set up with a default installation of an open-sourced project management tool and was ultimately forgotten about as work that was more important came up. The server, listening on a publicly-facing interface for easy remote access, was a soft target compromised by a simple brute force. Due to its connection to the domain and a credentials file left on the file system, the threat actors were able to use this server as a foothold to compromise other systems within the environment.

Lessons learned

Situations considered "unknown unknowns" are by far the hardest in which to plan and to react. Unfortunately, these represent a large number of breaches as the complexity and size of modern networks makes it difficult to always know what problems may exist. The varied and unpredictable nature of these types of incidents means that a robust set of options needs to exist to prevent and respond to unknown threats.

Mitigation

- Know all your assets and any critical data residing on those assets.

- Do not allow direct ingress or egress internet connections; implement proxies, where possible.

- Implement multi-factor authentication for access to all critical systems.

- Limit direct access to critical assets to restricted users and IP addresses only.

- Enable and centralize logging in a way that is easy for analysts to access during an incident.

Response

- Create IR Playbooks for data breach and other cybersecurity incident response.

- Change admin passwords immediately.

- Enhance logging by using packet capture or endpoint detection technology; analyze these logs to identify malicious traffic patterns.

- Supplement monitoring with proactive and freeform review to prevent tunnel vision.

- Engage legal and public relations teams early on.

Proactive review a.k.a. "threat hunting"

Fighting cybercrime is quickly becoming a nightmare for all organizations in an environment of moving targets. There are already many issues to manage as far as security threats are concerned and it's a constant challenge to manage the known vulnerabilities, let alone the unknown ones. Among a myriad of potential problems, it is critical for organizations to be aware of their assets, vulnerabilities, including network access permissions, and any countermeasures in place to thwart known threat actors and suspicious behavior. This scenario focuses on one such oversight, which cost a customer who was a leading player in the online gaming industry.

Proactive review is becoming a fundamental requirement for securing environments against unknown threats. Unlike signature-based technology, this type of review is built on analysts doing what they do best – finding strange or unexpected events on top of a baseline of expected behavior. Typically, these suspicious events are identified in high-fidelity data sets such as full packet capture or endpoint detection reporting, as greater depth in data allows the analyst to pursue leads and make a sound determination.

When combined with traditional monitoring, free-form review can be a very powerful safeguard against the unknown. It is unrealistic to expect manual analysis, often heavily dependent on the specific analyst conducting the review, to be either comprehensive or perfectly consistent. By offloading alerting and monitoring to intrusion detection systems or anti-virus solutions, the analysts can be allowed to focus exclusively on the types of events missed by these technologies.

This proactive approach to looking for potential threats relies heavily on context about the environment and analysts need time to become accustomed to the specifics of any new data sets. Over time, interaction with the data and answers to questions about the data allow a knowledge base to form and reduces the analysis time required in the long term. Creating documentation or striving for a homogenous environment can reduce the time required for new analysts to become familiar with a location.

The Way Forward

And, so we come to the end of this year's DBD: "Perspective is Reality." Let's look at five "overall" incident response tips and touch base on some takeaways specific to each Clustered Grouping.

Aside from "knowing your IR role and the associated responsibilities," which is obviously paramount, from our extensive field experience in responding to data breaches (and conducting proactive IR capability assessments), here are five key data breach response tips for every IR stakeholder to keep in mind:

1. Preserve evidence; consider the consequences of every action taken.

2. Be flexible; adapt to evolving situations.

3. Establish consistent methods for communication.

4. Know your limitations; collaborate with other stakeholders.

5. Document actions and findings; be prepared to explain them.

And we will round out our list of tips with some overall takeaways specific to each Clustered Grouping:

Clustered Grouping	Takeaway
The Human Element	• Know the threat actors; recognize their methods. • Know your employees; sensitize them to threat actor tactics and techniques. • Train your IR stakeholders to respond as a team.
Conduit Devices	• Know your devices; monitor and log activities. • Reduce their exposure through patching.
Configuration Exploitation	• Know your systems; configure them properly. • Patch and patch often; review code and configurations. • Conduct security and application scans regularly. • Know your network environment; segment and configure it properly.
Malicious Software	• Know the threat actor tools and capabilities; adjust your defense accordingly. • Employ File Integrity Monitoring; keep anti-virus updated.

We hope you enjoyed our publication and picked up a new perspective or two on data breaches. Until next time, we'll leave you with one final piece of Sun Tzu insight…

"There are not more than five musical notes, yet the combinations of these five give rise to more melodies than can ever be heard." – Sun Tzu

Appendix A: Key Incident Response Stakeholders

Incident Response (IR) stakeholders typically fall into two groups: internal stakeholders and external entities. Internal stakeholders consist of management and "hands-on" technical incident responders. External entities consist of a wide variety of experts advising and providing support to the internal stakeholders.

Every organization is different, and every organization is different when it comes to incident response and who its IR stakeholders are. These stakeholders range from Executive Management, who make final decisions on cybersecurity IR courses of action, to end users, who often represent the first line of defense for data breaches.

Internal IR Stakeholders

Internal IR Stakeholder Role	IR Responsibility
Chief Information Officer (CIO)	Responsible for enterprise IT strategy, networks, systems, and applications for an organization.
Chief Information Security Officer (CISO)	Manages information security implications, to include strategic goals, personnel allocation, infrastructure implementation, policy enforcement, emergency planning, cybersecurity awareness and other activities.
Legal Counsel	Provides legal advice and recommendations on cybersecurity incidents and response activities.
Human Resources	Provides guidance and assistance for cybersecurity incidents involving employee activity or employee Personally Identifiable Information (PII) related breaches.
Corporate Communications/ Public Relations	Manages internal and external communications related to cybersecurity incidents.
Incident Commander	Leads the Tactical IR Team; see "Tactical IR Team Members".
Information Technology (IT)/IT Security Team	Manages IT Team and IT security aspects (e.g., applications, systems and network).
Physical Security	Assesses the impact of physical aspects of cybersecurity incident.
GRC/Internal Audit	Evaluates IR Plan for governance, risk, and compliance purposes.
Data Loss Prevention	Monitors, detects and blocks sensitive data at-rest, in-use or in-motion.
Business Continuity	Implements Business Continuity Plan and business continuity capabilities to maintain critical business functions during cybersecurity incidents.
Disaster Recovery	Implements Disaster Recovery Plan and data recovery capabilities to recover from cybersecurity incident-related disasters.
Help Desk/Customer Support	Receives and communicates cybersecurity incident-related information.
End Users	Serves as first line of cybersecurity defense; an incident detection trigger.

Tactical IR team members

IR Team Member Role	IR Responsibility
Incident Commander/IR Team Manager	Leads the tactical IR Team by providing direction and guidance; represents the tactical IR Team during stakeholder meetings; updates stakeholders on response progress.
SOC Analyst	Monitors for and initially responds to cybersecurity incidents.
SIEM Technician	Manages and leverages response and analysis capability of network/application Security Incident and Event Management (SIEM) tool.
EDR Technician	Manages and leverages response capability of Endpoint Detection and Response (EDR) tool.
Internal Investigator	Conducts investigations into allegations of employee misconduct.

External entities

External Entity Role	IR Responsibility
Digital Forensics Firm (e.g., Verizon RISK Team)	Supports the Tactical IR Team with digital forensics investigation activities, including collecting, handling and analyzing evidence.
Law Enforcement	Investigates cybersecurity incidents involving criminal activities; possible source for data-breach-related information.
Security Vendor(s)	Provides advice and assistance on deployed tools and systems related to cybersecurity and/or response activities.
Data Storage Vendor(s)	Hosts and stores data, backups and/or log data.
Internet Service Provider(s)	Provides internet connectivity.
Cyber Insurance Carrier	Provides insurance for data breach and other cybersecurity incidents.
Outside Counsel	Supports internal Legal Counsel with specialized legal advice.
External Public Relations Firm	Supports internal Corporate Communications/Public Relations.
US-CERT/Regional CERTs	Responds to cybersecurity incidents, analyzes threat actions and shares cybersecurity information with partners.
Industry ISACs	Shares physical and cyber threat and vulnerability information.
Payment Card Brands	Provides information relevant to payment card breaches to include proactive and reactive security and response activities; develops and enforces its own programs regarding when and how PFI investigations may be required.
Payment Card Acquirers	Enter into agreements with merchants to accept and comply with Payment Card Brand operating rules and procedures.

Appendix B: CIS Critical Security Controls

The 20 Center for Internet Security (CIS) Critical Security Controls (CSCs) – Version 6.1:[9]

CSC #	Critical Security Control
CSC-1	Inventory of Authorized and Unauthorized Devices
CSC-2	Inventory of Authorized and Unauthorized Software
CSC-3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC-4	Continuous Vulnerability Assessment and Remediation
CSC-5	Controlled Use of Administrative Privileges
CSC-6	Maintenance, Monitoring and Analysis of Audit Logs
CSC-7	Email and Web Browser Protections
CSC-8	Malware Defenses
CSC-9	Limitation and Control of Network Ports, Protocols and Services
CSC-10	Data Recovery Capability
CSC-11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches
CSC-12	Boundary Defense
CSC-13	Data Protection
CSC-14	Controlled Access Based on the Need to Know
CSC-15	Wireless Access Control
CSC-16	Account Monitoring and Control
CSC-17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC-18	Application Software Security
CSC-19	Incident Response and Management
CSC-20	Penetration Tests and Red Team Exercises

9. www.cisecurity.org/critical-controls/Library.cfm

VerizonEnterprise.com