Fidelis™ Cybersecurity

Shutting the Door on the Attacker

Case Studies in Kicking Advanced Adversaries Out of Your Network

www.fidelissecurity.com

Contents

Introduction

The knee-jerk reaction when you learn that you have been compromised is understandable: get them out. Think about what you would do if you came home and saw burglars in your house. You would call the police. Immediately! But when it comes to computer security, it can be counter-productive to act too soon.

If all you have seen is a spear phishing email or isolated command and control activity, you may just be looking at the tip of the iceberg. If you act too soon you could alert the attacker and they might entrench themselves in ways that are hard to detect. On the other hand, if you wait too long, the attackers could steal critical data.

What should you do? And when should you do it?

These are questions we get asked every time we respond to a security incident. And the answer is almost always a frustrating one: "It depends."

Just as a doctor has to examine a patient before prescribing a course of treatment, we need to investigate and fully understand the scope of an incident before we can determine the most effective approach for kicking the attackers out and keeping them out.

About This Document

In this document we outline key questions to consider when you are deciding how and when you should expel attackers. We outline two specific expulsion approaches along with case studies of specific expulsion scenarios based on security incidents our consulting team has investigated.

Expulsion Is the End...Not the Beginning

A successful expulsion event is the culmination of a thorough investigation and thoughtful planning. You can only effectively expel the attacker once you fully understand the scope of the incident you are dealing with and develop a detailed plan to execute an event.

You will never have perfect information about any incident, but here are some of the key questions you will want answers to before you formulate a plan for kicking the attackers out:

- Where are the attackers in your environment?
- How long have they been there?
- How are they maintaining access?
- What is their motive?
- What systems, applications and user accounts have they compromised?
- What command and control mechanisms are they using?
- What existing security controls are in place?
- How did the attackers circumvent these controls?
- Are there tools in place to detect and respond if they come back?

Whilst the specific steps of an investigation will differ depending on the nature of the incident and the organisation's size, structure and line of business, there are four general phases. The table below outlines how the Fidelis security consulting team approaches an incident.

Four Phases of Incident Response

Phase 1 Initial Response	Phase 2 Investigation & Containment	Phase 3 Expulsion	Phase 4 Remediation
• Determine the current status of the investigation • Get situational awareness by assessing existing security controls, defence-in-depth strategy, current technology and staffing • Determine the scope and level of effort required to perform incident response	• Investigate to identify the who, what, when, where, why and how of the incident • Identify the attackers and their tactics, motivations and actions • Control or eliminate the intruder's access to critical resources	• Remove the intruder's ability to perform any action within the environment • Remove all attackers' tools and files • Return the environment to its normal state prior to the incident • Monitor to ensure the attacker does not return for a period of time	• Evaluate the environment to ensure the attacker has not returned • Recommend actions to prevent the attacker from re-establishing access • Recommend a short- and long-term roadmap to enhance the organisation's IT security posture

Planning for a Successful Expulsion

When you decide you are ready to boot the attackers out, two things are critical. You have to be comprehensive. And you have to move fast. That takes planning.

Do It Once. Do It Right.

Attackers know they will be discovered at some point. Their goal is to survive and persist in your environment throughout your expulsion process. To succeed they use multiple tactics and techniques to infiltrate your network and establish a foothold. It's critical that when you begin your expulsion you have thoroughly identified the attacker's command and control systems during your investigation so you can remove them and eliminate the attacker's ability to operate in your environment.

Timing is critical. If you start the expulsion process before you have fully scoped the incident you may alert the attackers that expulsion activities are underway. The attackers may go quiet and then use an undiscovered backdoor to return at a later date. If attackers have destructive motives, tipping them off also runs the risk of causing them to take destructive action against the organisation.

It's critical that when you begin your expulsion you have thoroughly identified the attacker's command and control systems during your investigation so you can remove them and eliminate the attacker's ability to operate in your environment.

Speed Is of the Essence

If the expulsion event goes according to plan, the attacker will wake up one morning and find that all of the doors they were using to infiltrate your environment have been simultaneously closed and locked. Achieving that outcome requires executing your expulsion plan in as short a time-frame as possible — usually within 72 hours or less. In fact, expulsion events often take place over a weekend — both because the attackers may not be "working" and because it usually minimises disruption to ongoing operations.

The critical areas to focus on during an expulsion event are:

- **Locking Down the Perimeter.** By blocking malicious IPs on the firewall you can disrupt the attacker's command and control and ingress/egress capabilities.
- **Updating Anti-Virus Signatures.** Implementing custom signatures based on the tools and malware you have seen attackers use in your environment will help actively defend your endpoints.
- **Resetting Credentials.** By resetting passwords to compromised (or sensitive) accounts you can deny attackers privileged access to the Active Directory domain and VPN connectivity; and disrupt the attackers' ability to authenticate.
- **Remediating Endpoints.** Removing malware and exploit kits, reimaging hosts and rebuilding compromised systems ensures endpoints are free of attackers. Hosts that cannot be reimaged will need expulsion scripts executed, with the intent of removing all malicious code whilst preserving the machine state.

Unfortunately, most organisations' networks are not simple and straightforward. Larger organisations will have multiple points of presence (PoP) to the Internet and multiple modes of connectivity (e.g., DSL, private MPLS) and/or involve outsourced third parties like managed security services providers (MSSP). All of this can further complicate the process.

Choosing the Right Expulsion Approach

There are two primary approaches to kick attackers out. Both methods have their advantages and disadvantages. In order to figure out which one suits you best we recommend asking yourself the following questions:

- What level of risk am I willing to accept?
- What internal resources are available to support the investigation and expulsion?
- What is my tolerance for hiring external incident response consulting services?
- What are my legal risks and responsibilities (e.g. public reporting requirements)?
- Have law enforcement agencies made requests to leave the attackers in the network until they obtain more evidence?
- Does my incident response plan outline specific expulsion procedures?

Approach #1: Reactive Expulsion

In short, the reactive expulsion approach involves taking action as soon as you identify compromised machines or attacker activity. Whilst it is hard to fully expel attackers using the reactive approach, it is frequently employed when organisations face an imminent threat or lack the resources to fully staff a comprehensive expulsion. For example, let's say you observe active data theft of personally identifiable information (PII). Or, perhaps you have identified the attacker has compromised the CEO's email account. In both cases you would be justified in acting immediately — even before you have completed your investigation.

In situations that call for a reactive expulsion, the response team quickly adjudicates suspicious activity as known bad or known good and immediately blocks or removes points of infiltration and exfiltration as they discover them. As a result, the short-term cost to the organisation is often lower than with a coordinated expulsion. However, the need to act without a full understanding of the incident's scope can leave the door open and allow attackers to persist or re-compromise your environment. Also, the whack-a-mole cycle of search, analyse and eradicate can be disruptive to business operations and frustrate users.

In short, some of the drawbacks of this approach include:

- There is less time to adjudicate suspected attacker activity
- Attackers could go quiet and return later
- Investigative efforts may miss non-beaconing backdoors
- The lack of visibility into attackers' movements in real-time may result in not fully understanding their tactics and motivations
- Personnel assigned to investigation may need to be diverted to expulsion activities.

REACTIVE EXPULSION:

Multinational Computer Services Firm Expels Attacker Targeting Their Clients' Networks

The Situation

Fidelis was called in to assist a multinational computer services firm with an attack that posed an immediate threat to them and their clients. Despite responsible and sustained investments in a defence-in-depth strategy, the attacker gained entry to the organisation's network through its clients' networks.

When we engaged, we observed the attacker pivoting to move laterally through the network in order to penetrate the networks of other clients. The attacker used administrative credentials to disguise their malicious actions as routine network traffic and move undetected through the network.

Based on the attacker's tactics and the sophistication of the malware they were using, we determined that they needed to get real-time visibility across both the network and endpoints.

The Investigation

We deployed a suite of advanced network monitoring and host-based investigative tools to aid their investigation. The enhanced network visibility enabled us to rapidly sweep the environment for indicators of compromise (IOCs), such as filenames and hash values of files, so they could identify "hosts of interest." We uncovered attacker activity beyond the original scope of the investigation, including malware camouflaging itself as normal system processes, using DLL injection techniques and other means, and encrypted communications with malware infected servers over non-standard ports and protocols.

When we engaged, we observed the attacker pivoting to move laterally through the network in order to penetrate the networks of other clients.

The Expulsion

The forensic evidence allowed the Fidelis incident response team to develop a remediation plan that included deploying kernel-level malware detection software in a surgical fashion to remove the attackers and their tradecraft as they found them. In addition to successfully expelling the attackers, the counter measures prevented the escalation of privileges on Active Directory privileged accounts.

Following the expulsion events, we continued the enhanced security monitoring to support post-remediation actions and guard against persistent and re-entry attacks. The attacker tried multiple times to re-establish a foothold into the customer-facing and corporate networks. The attacker also tried to elevate administrative privileges through different attack vectors, but all attempts were discovered, preventing their access to do further harm.

REACTIVE EXPULSION:

Energy Firm Shuts Down Command and Control Communication

The Situation

A U.S.-based energy firm engaged the Fidelis incident response team to assist with an active attack. When we arrived, the client was already fully engaged with the attacker and was blocking their command and control IP addresses at the firewall.

Since the attackers were well aware that the company knew it was compromised, we determined that the risk of further compromise or damage by the attacker warranted an immediate reactive expulsion.

The Investigation

The team stood up three workstreams for security monitoring, expulsion and recovery. As investigators found new malware, they worked to quickly understand its behaviour and how the attacker was using it. Then, they quarantined or removed it. Unfortunately, the investigators discovered that the attackers were also using legitimate administrator tools. Quarantining these tools was not an option because network administrators needed access to the same tools.

Since the attackers were well aware that the company knew it was compromised, we determined that the risk of further compromise or damage by the attacker warranted an immediate reactive expulsion.

During the investigation, we found malware that pulled usernames and passwords. We initiated a full password reset. Then, several weeks later, we found different malware that also pulled usernames and passwords. Because the new malware was unknown when the attackers used the second set of malware, we initiated another password reset. Whilst it was the "safe" thing to do, it came at the expense of frustrating employees who were forced to reset their passwords multiple times.

The Expulsion

The expulsion efforts shut down the inbound and outbound communication based on attacker IP addresses. Whilst the attackers tried to get back into the network by exploiting vulnerabilities on the exterior of the network, their efforts were effectively blocked. This provided relief to the client as it indicated that the attackers did not have additional backdoors planted in the network.

Although the attacker retained some of their capabilities since the client was unable to quarantine the administrator tools, the client significantly minimised their risk going forward by mitigating the attacker's tools and access as they were discovered. Whilst the urgency of the situation called for reactive expulsion, the client plans to choose the coordinated expulsion approach for future incidents.

Approach #2: Coordinated Expulsion

In the majority of incidents we respond to, the attacker has been active in the victim's environment for several months. They are deeply entrenched and have multiple persistence mechanisms in place. Assuming there is not active theft of sensitive data, we typically recommend a coordinated expulsion approach. What this means, in practice, is that we perform a thorough investigation until we feel comfortable that we understand the scope of the attack at a level that we believe we can fully eliminate the attacker's ability to access or cause damage in the network.

The coordinated expulsion approach is generally more effective at kicking attackers out and keeping them out with a single event. However, it assumes that you are willing to accept the risk of watching and observing attackers in your environment whilst you formulate your expulsion plan. It also assumes that you have (or can hire) the resources to complete a thorough investigation and execute the expulsion event on a tight timeframe.

When the coordinated expulsion occurs, incident responders identify and flag the attackers' movement, methods of communication, malware and exploited tools for removal at a specific time. A benefit to executing a coordinated expulsion event is that the investigation team has more time to adjudicate suspected attacker activity and gains considerable knowledge of the attackers' tactics and motivations. This provides the team with a more complete picture of the scope of the attack.

Disadvantages to coordinated expulsion include:

- The cost to the organisation is often higher than reactive expulsion
- There is a higher risk that the attackers may identify expulsion activities and cause malicious damage
- There is a higher risk that the organisation may lose data.

COORDINATED EXPULSION:

Large-Scale Coordinated Expulsion Defeats Advanced Attacker Targeting Active Directory

The Situation

In nearly every case Fidelis investigates, attackers look for ways to steal valid user credentials and escalate their privileges. In this case, Fidelis was called in to investigate an incident where the attacker had done just that. They compromised the client's Active Directory identity and access management (IAM) system installed throughout the global wide area network. Then, the attacker installed malware onto hosts and used it to harvest account credential hashes and data. This, in turn, allowed the attacker to masquerade as authorised and privileged users, further escalate privileges and access sensitive data.

The Investigation

The existing detective controls the client had in place did not provide adequate information about the attacker's activity. It was clear that the attacker was deeply entrenched. Since we knew we were dealing with an advanced adversary that had extensive and longstanding access to the environment we determined that any attempt to remediate the environment or expel the attacker without fully understanding their capabilities would result in failure and expose the client to higher risk. Successful resolution required a phased approach to remediate the vulnerabilities the attackers were exploiting.

The ability to differentiate malicious traffic from normal, administrative network traffic and host activity was vital for successful remediation. To gain situational awareness, increase overall visibility and facilitate intensive data analysis, the response team set up a security operations centre (SOC) using network-monitoring tools and staff to monitor and report on identified attacker activity.

The continuous network monitoring allowed the response team to:

- Scope attacker movements
- Track and isolate compromised assets for remediation
- Determine the extent of exposure
- Plan for attacker expulsion.

During the investigation we identified that the attacker had created an operational environment that they could access "at will." They deployed and periodically updated customised tools that were undetectable by anti-virus software. They used encryption and established user accounts, including enterprise and domain administrator credentials to reconfigure hosts and bypass authentication requirements of the host operating system. Finally, they exploited existing proxy devices at internet points of presence for exfiltration.

We knew we were dealing with an advanced adversary that had extensive and longstanding access to the environment.

The Expulsion

The ability to "see" activity occurring on the global wide area network was vital to successfully resolving this incident. The SOC team's network monitoring and data analysis — during both the investigation and expulsion event — was critical to short- and long-term remediation planning. It provided the incident response team with the confidence to schedule and execute the coordinated expulsion and remediation activities.

Once the expulsion was complete, ongoing network monitoring established during the investigation phase allowed the response team to:

- Ensure expulsion and remediation tasks were successfully executed
- Determine the effectiveness of identity and access management
- Verify that known attacker movements and tactics were no longer occurring in the environment
- Identify the attackers' attempt to re-enter the environment.

The security controls provided by network- and host-based monitoring tools continue to play an important part in the overall enhanced security architecture within the firm's global IT infrastructure.

The detective tools that were loaded with every available threat intelligence product pertaining to the attackers are regularly updated and provide a level of vigilance for any event occurring post-expulsion, through the use of log and network packet capture and query technology.

COORDINATED EXPULSION:

Transportation Firm Executes Comprehensive Expulsion Flawlessly and Ahead of Schedule

The Situation

A transportation firm contacted Fidelis to help them investigate a suspected incident. We quickly identified that the adversary was an advanced attack group that had been operating in the victim's environment for several months. The company elected to pursue a coordinated expulsion because they understood that they needed to learn as much as possible about the attackers before they tried to kick them out. No attacker activity had been observed during the months prior to the incident response so ongoing data theft was not a concern. Nevertheless, investigators cautioned the client that the absence of observable attacker activity didn't mean that attackers were not in the network.

The Expulsion

Following the investigation, the teams planned a full-scale expulsion event that would span 72 hours. The planning included:

- Removing affected systems
- Removing known malware and tools used by the attacker
- Resetting all user credentials
- Blocking known bad IP addresses.

The company elected to pursue a coordinated expulsion because they understood that they needed to learn as much as possible about the attackers before they tried to kick them out.

The investigation team swept all systems on the network and followed the attackers' trail through every affected system. Two weeks prior to the scheduled expulsion, they were confident that they knew where the attackers had been and what they had done. Likewise, the containment team understood what parts of the network were vulnerable and how the attackers were communicating inbound and outbound on the network.

Leading-up to the expulsion event, the containment team updated all of the relevant security tools with indicators of compromise (IOCs) gleaned from the investigation. These were loaded into antivirus, proxies, email monitoring tools, SIEMs, firewalls, edge network communication monitoring tools and IDS/IPS devices. Equally important, the password reset team had a phased approach on resetting Active Directory users, local system user accounts and local system administrator accounts.

Prior to the expulsion event, the teams met in a large training conference room to perform a mock tabletop exercise to run through the event. These exercises proved invaluable and the expulsion event occurred without any major issues.

The team had allocated five days for the expulsion event. But, in the end, they finished ahead of schedule and completed all tasks within 72 hours.

Whilst most systems and user accounts in the organisation were impacted by the expulsion event, the team achieved its key success criteria of eradicating the attacker without impacting operations. In the end, not a single operational system went down as a result of the changes the team made on the network.

Conclusion

Security incidents can be stressful. But it's important to think before you act. Every action you take will elicit a reaction from the attacker, so the more knowledge you have before you act the more successful you will be in kicking the attackers out and keeping them out. Reactive expulsions and coordinated expulsions are two solid options. The important thing to remember is that each organisation and each incident is unique and requires a slightly different approach to achieve a successful outcome.

Fidelis Cybersecurity is creating a world where attackers have no place left to hide. We reduce the time it takes to detect attacks and resolve security incidents. Our Fidelis Network™ and Fidelis Endpoint™ products look deep inside your traffic and content where attackers hide their exploits. Then, we pursue them out to your endpoints where your critical data lives. With Fidelis you'll know when you're being attacked, you can retrace attackers' footprints and prevent data theft at every stage of the attack lifecycle. To learn more about Fidelis Cybersecurity products and incident response services, please visit **www.fidelissecurity.com** and follow us on Twitter **@FidelisCyber**.