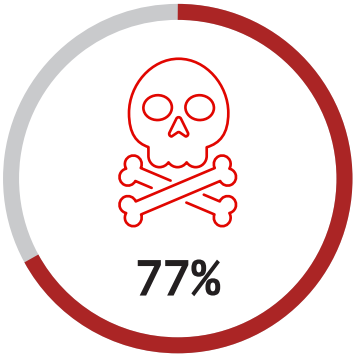
MANDIANT

WHITE PAPER

ENEMIES IN OUR MIDST

Why security-conscious organizations use Compromise Assessments



of organizations surveyed experienced at least one successful cyber attack in 2018

$2.1 trillion

is the estimated total cost of cyber crime in 2019

$3.5 million

is the projected global workforce gap for 2022

Executive Summary

Almost every week we hear a tale of yet another company getting attacked. It's not if your organization will be breached—it's when.

And most attackers are active in environments for a significant amount of time before being discovered. In 2018, organizations in EMEA were not aware of the attacker in their midst for a median of 177 days.[1]

Added to that, only 56% of these organizations detected the breach. External entities notified 44% of organizations they'd been successfully attacked. Once inside, advanced attackers have near free rein.

This is where a compromise assessment can help.
A compromise assessment answers the all-important question: Have you been breached?

Typically, you would employ a third-party expert to do a compromise assessment of your environment because of the specialized expertise, intelligence, and technology required.

This combination of skills and tools are only found in non-technical senior executives and a report body with sufficient technical detail to enable security technicians to act on the information provided.

The compromise assessment report provides you with multiple benefits. First, if you haven't been compromised, you get the peace of mind of knowing that a firm

that specializes in detecting malicious activity did not find any in your environment. You also get strategic recommendations based on the assessment firm's experience working in your environment and general experience responding to advanced attacks.

If you have been compromised, you already have an expert team at hand which can respond to the incident with technology already deployed. And in either case, you're following best practices for a mature security program.

> By identifying a particular attacker or type of attacker, an assessment team with specialized intelligence is better able to understand the motivations and goals of the attack.

1 1 Mandiant. M-Trends 2019: By the Numbers. 2019

Introduction

There's no such thing as 'secure' anymore," Debora Plunkett, a director of the National Security Agency (NSA) said after a particularly embarrassing WikiLeaks incident.[2]

Plunkett heads the NSA group responsible for protecting national security information from the battlefield to the White House. She recommends a proactive strategy that many security experts have advised for years: Assume you've already been compromised, and manage your environment accordingly.

But what does this mean? A vital first step is assessing whether you have been compromised. Even the most secure organizations routinely commission such assessments because attacks evolve, and corporate security cannot always keep up. An attacker only needs to exploit a single vulnerability to gain a foothold in an organization whereas corporate security has to worry about every vulnerability in their environment.

A compromise assessment is also a good way to make sure that your security controls are operating as expected. Finally, an assessment can notify you of a breach before an external third party without your best interest at heart does. If the assessment does discover a breach, you can move into full-scale IR mode and immediately begin investigating and remediating.

But even if you haven't been compromised, such assessments are worth your time. You get a clean bill of health that allows you to sleep easier at night. And you have something tangible for your chief information security officer (CISO) or chief information officer (CIO) to give to the executive board or shareholders that provides them with confidence in your security program.

In this white paper, we'll explain what it means to assess your environment for evidence of compromise. We'll tell you what to expect from such an assessment. Finally, we'll help you understand how to get started.

Once a target, always a target

Last year's M-Trends reported that in 2017, 56% of FireEye managed detection and response customers who were previously Mandiant incident response clients were targets of at least one significant attack in the past 19 months by the same or similarly motivated attack group. In 2018, this number has continued

to climb, increasing to 64%. This data further substantiates the fact that if you've been breached, you are much more likely to be targeted again and possibly suffer another breach.

Region	2017	2018
Americas	44%	63%
EMEA	47%	63%
APAC	91%	78%
Global	56%	64%

FIGURE 1. Retargeted incident response clients, by region.

2 Jim Wolf December 16,2010. "U.S. code-cracking agency works as if compromised."

Lifecycle of a Targeted Attack

Advanced attack groups—which are typically backed by organized crime syndicates or governments—have started to more openly target public and private sector organizations. Their goal: To steal data, frequently over extended periods of time.

To achieve this, they implement tools, techniques, and procedures (TTPs) designed to evade detection. They develop custom malware and use techniques that blend in with normal user and system activities. And they try to fly under your radar so that they can operate in your environment for months or years. This is why assessing whether you've been compromised is important even if you've deployed a strong portfolio of security products.

The attack lifecycle (see Figure 1) can be applied to any breach. And detecting evidence of a compromise can be performed at any stage throughout the lifecycle.

Let's assume an attacker sends a spear-phishing email with a malicious link that downloads malware (the initial compromise) and installs a backdoor (establishes foothold). The attacker then connects to the backdoor, executes a tool to steal password hashes of the local

administrator account (escalates privileges), and executes commands against Active Directory to understand group membership (internal recon).

Armed with this knowledge, the attacker targets domain administrator systems (moves laterally), gains access to domain administrator credentials (escalates privileges), and installs a web shell on an Internet-accessible web server (maintains presence). Finally, the attacker leverages the harvested credentials to extract, stage, and steal executive email (completes mission).

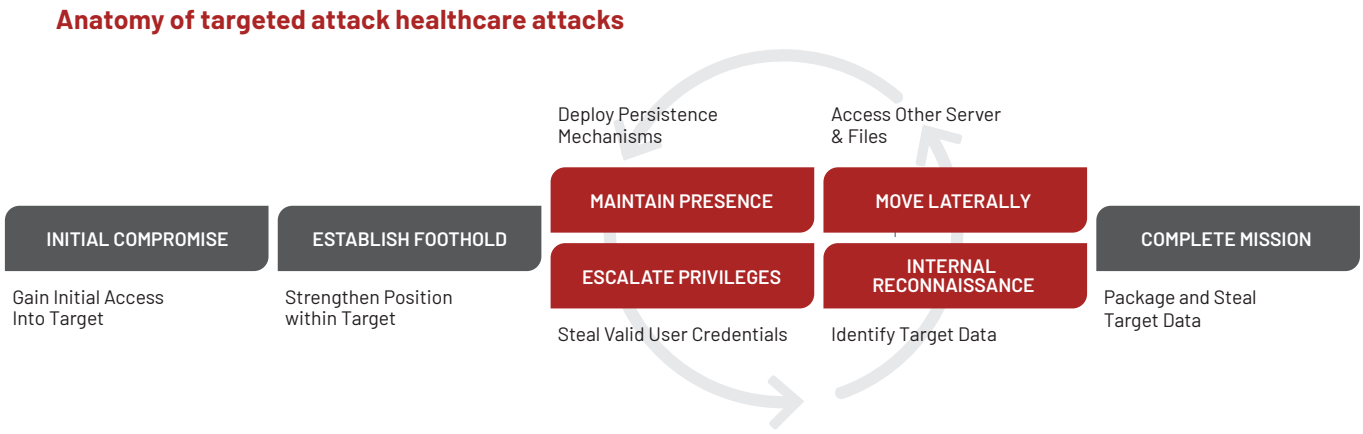


FIGURE 2: Lifecycle of a targeted attack

> Assessing whether you've been compromised is important even if you've deployed a strong portfolio of security products.

THE STAGES IN THE ATTACK LIFECYCLE

- **Initial compromise**
  The attacker gains access to the target organization's network or systems.
- **Establish foothold**
  The attacker gains remote control over a system within the victim's environment and establishes a persistent presence.
- **Escalate privileges**
  The attacker compromises legitimate credentials and escalates privileges, often to domain administrator, local administrator, or even the network root. These user accounts provide access to more systems and data.
- **Internal recon**
  The attacker identifies critical assets (data, people, and systems) of interest.
- **Move laterally**
  The attacker accesses systems throughout the environment to advance the attack.
- **Maintain presence**
  The attacker employs various techniques to remain in the victim's systems and networks.
- **Complete mission**
  The attacker accomplishes the goal, which is typically to steal data.

The activities described above leave trace evidence at all stages of the attack lifecycle. Compromise assessments are designed to find that evidence. There's the browser history of "patient zero"—the first phishing victim—the evidence of malware and the persistence mechanism on patient zero's system, or the anomalous use of the local administrator and domain administrator accounts to move laterally through the environment. There's also the presence of the web shell. Finally, it should find evidence of the tool used to bulk extract the targeted email, the compression utility used to stage the data, and whatever method the attacker used to transfer the data out of the environment (just to name a few simpler traces of evidence).

Any or all of this may fly under the radar of your standard security detection devices, but a compromise assessment is designed specifically to look for this type of activity.

How to Identify a Compromise

Some focus areas for a compromise assessment firm:

Reused custom malware. Commercial malware is widely available to buy on the dark web. Still, many attack groups—particularly those involved in targeted attacks—will go to great expense to develop custom malware. Naturally, they prefer to reuse it to protect their investment.

Or they modify it slightly to create variations to avoid detection. An experienced compromise assessment team can detect attack groups by matching the "fingerprints" of such malware identified during prior investigations.

Unique persistence mechanisms. Attackers use many techniques—some well known, others more obscure—to maintain a presence in your environment. For example, Windows registry entries can store malware execution parameters. Attackers might place malware in a Windows startup folder. Or they might hijack legitimate system binaries with Trojan malware. Knowing how attack groups commonly operate allows the assessment team to detect signs that a breach is in progress or has recently occurred.

Lateral movement techniques. Most advanced attack groups compromise legitimate credentials to mimic standard user behavior. They then use the compromised credentials to move freely through an environment.

An experienced assessment team understands how attackers typically obtain and use those credentials. For example, attackers use common utilities to steal passwords. The team will also be familiar with signs of malicious lateral movement through an environment.

Reuse of network indicators. Attack groups often reuse website domain names, IP addresses, web security certificates, and network protocols across many victims. An experienced assessment team immediately flags such uses. The team may even be able to decode or decrypt the network traffic to see the commands the attacker is issuing.

Malicious attacker activity. An expert assessment team has many collective years of experience finding the most difficult-to-detect advanced threats. They not only can detect the malware (this is usually the easy part), but also other evidence of attacker activity such as what the attacker did when inside the environment. The team should have many analytical techniques in its arsenal to find the proverbial needle in the haystack.

What You Get at the End of a Compromise Assessment

When the assessment team is done, you get a comprehensive report that you can share with senior executives and technical staff. The report should consist of an executive summary written at a high level so that non-technical senior executives can easily digest it. At the same time, the report should contain enough technical detail to enable security technicians and analysts to act on the information.

The executive summary should include background information on why you commissioned the assessment and high-level details of the approach taken. The executive summary should also clearly state the bottom- line results: Have you been compromised? If you have been, the results should include intelligence on the attack group(s), the malware found, the assets compromised, and other useful statistics.

The body of the report should contain sufficient technical detail to support the executive summary. If a compromise is detected, each aspect of that compromise should be explained so that security personnel can understand its severity. The body should also include recommendations for next steps. For compromised organizations, the next step is almost always launching IR.

A sometimes-overlooked aspect of a good assessment team is how easily it can transition from the assessment into IR in the event that an attacker is found in the environment.

If no compromise is detected, the report should focus on the completeness of the assessment. It should explain the analysis techniques used to assure you (and your management) that the assessment was thorough and that your organization had a clean bill of health at the time of the assessment, based on the information provided and the attacker TTPs known at that time.

Benefits of a Compromise Assessment

You might want an assessment for many reasons. The most typical ones are the board wants to know if they have been breached or an organization in your industry has been breached and you're worried about your own environment.

It's not unusual for advanced attack groups to target multiple companies in multiple industries using the same techniques. So hearing of other attacks, even from different industries, is often the trigger for organizations to see whether they, too, are victims.

You receive benefits even if a compromise was not discovered:

- **Get peace of mind.** You get independent validation that your assets have not been breached. You can communicate this good news to executives, shareholders, customers, and compliance professionals.
- **Establish a baseline.** You get a refresh point of "known good" that you can refer to should you detect any suspicious activity in the future.
- **Access the latest threat intelligence.** This should include what's happening in your industry as well as the security world in general.

Another benefit is that if you have been compromised, in addition to knowing about it, you already have a vendor capable of responding to the threat working in your environment. In such cases, the assessment team can start investigating the breach immediately.

The Mandiant Approach

Mandiant, has long been on the front lines of helping organizations prepare for and respond to security breaches. Here's how we leverage our intelligence, expertise, and technology to thoroughly assess organizations for compromise.

Deploy network and host-based inspection technology

Mandiant Consulting uses advanced technologies that leverage signature and analytical methods for detecting malicious activity. Our methodologies ensure that "unknown" malware can be detected as well as attacker activity where malware is not present. Detecting known malware is easy. Detecting unknown malware is the real challenge. Because of this, We uses proprietary technology at Internet egress points and on host systems such as servers, workstations, and laptops. All of the proprietary technology we deploy was built from an incident responder's perspective, having in aggregate responded to thousands of breaches.

Leverage intelligence from prior investigations

Mandiant Consulting possesses specific insider insight into the latest TTPs of advanced attack groups that includes detailed profiles of key attack groups, their tools, practices, and objectives, along with corresponding indicators of compromise (IOCs).

Our intelligence is much more than what is publicly available through the many online security publications. It consists of first-hand knowledge of attacker activity that is not publicly available. With this intelligence, we developed a detailed library of IOCs that use host-based artifacts and network traffic signatures to identify evidence of attacker activity. These IOCs are deployed throughout all our host and network-based tools.

Assess the environment for anomalies

Performing an assessment requires detective-like skills for detecting and analyzing clues. Mandiant comprehensively analyzes data along all phases of the attack lifecycle to trace an attacker's progress. We use knowledge of attack groups and analytical techniques developed from thousands of investigations to assess systems and network traffic for evidence of attacker activity. The focus is on detecting anomalous activity that stands out from the "accepted norm."

Analyze evidence

When Mandiant Consulting finds IOCs or anomalies, our consultants use skills that range from live response and forensic analysis to reverse engineering malware and network traffic analysis. We perform this analysis to confirm the findings and to better understand the severity.

Summarize findings

At the end of the assessment, Mandiant Consulting writes a detailed report that summarizes the steps taken, the major findings, and any recommendations.

Come Out Ahead with Compromise Assessments

At a time when cyber attacks are mounting year after year—with companies of all industries being targeted—the chances that you have been compromised are growing. But given the sophistication and agility of attackers, you often don't know you've been breached until weeks or—more likely—months later.

In such cases, having your environment assessed for indicators of compromise can be invaluable. The assessment will either notify you that you have (or had been) successfully breached or provide you with a clean bill of health at the time of the assessment. In either case, you come out ahead.

Your next steps should involve finding a third-party IR firm specializing in detecting as well as investigating and remediating breaches using the criteria set forth in this paper. Even if you have had an assessment previously that gave you the welcome news that you had not been breached, it makes sense to periodically revisit your environment with the help of experts to ensure that you remain that way. Ignorance may sometimes be bliss, but it rarely is for long when an attacker is active in your environment. We believe it's best to be sure.

Learn more at **www.mandiant.com/consulting**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT