Assessing Cybersecurity Risk in a Breached World

The Role of the Compromise Assessment

WHITE PAPER

Infocyte™

Table of Contents

Executive Summary

Our networks are attacked hundreds, sometimes thousands, of times a day by hackers and fraudsters throughout the world. Occasionally, these attacks are successful in gaining a foothold into the targeted networks. Worse, skilled attackers have demonstrated they can remain hidden for months, sometimes years, before detection once inside. When able to maintain long term (persistent) access like this, attackers are able to spy on operations; steal sensitive information; corrupt files; and even cause physical damage by manipulating industrial control systems (i.e. motors, actuators, or power).

According to industry reports, the average network security breach goes undetected for over 6 months (205 days).[1] In over two thirds of these cases, the breach is discovered by a third party such as law enforcement or investigative journalists.

According to industry reports, the average network security breach goes undetected for over 6 months (205 days).[1] In over two thirds of these cases, the breach is discovered by a third party such as law enforcement or investigative journalists. This problem is known in the security industry as the "breach detection gap" and it represents one of the greatest threats for organizations that do business with information technology.

This problem exists for two reasons:

1. The growing sophistication of modern attackers.
2. Current real-time security processes are ineffective at detecting post-compromise activity, especially as time passes after the initial attack.

Despite the threat of persistent compromises within our networks, information risk managers still rely on network assessments (i.e. vulnerability assessments and penetration testing) which only answer half of the question: "Can you be hacked?" With the growing need for confidentiality and data protection in the enterprise, information risk managers need the ability to quickly discover and address security breaches and then validate whether the network is, in fact, clean of unauthorized software and access. This "compromise assessment" compliments current risk and vulnerability management approaches by answering the more vital question: "Am I currently hacked?"

This white paper introduces the role and need for the Compromise Assessment, a new class of security assessment which seeks to identify unknown security breaches and adversary presence (i.e. malware, compromised systems, or malicious/unauthorized account use) within a network. It will also demonstrate how the latest "hunt" methodologies and technologies can be best applied to deliver a rapid and effective compromise assessment, giving information risk managers unparalleled fidelity and confidence into the status of their networks.

[1] Mandiant M-Trends 2015

Current State of Network Security Assessments

Network security and risk assessments are widely recognized as a key component of enterprise IT security. These assessments are used to measure and report on the health of the network and the risks associated with operating them. Currently, three types of network security assessments are regularly performed within enterprise:

1. **Compliance Assessment** – Identifies a network's state of compliance with various regulatory requirements and policies.

2. **Vulnerability Assessment** –
   Identifies known security weaknesses in targeted systems. Broadly, these assessments can be scoped in three ways:

   - *External* - Conducted from outside the network without access or prior knowledge of internal systems.

   - *Internal* - Conducted from inside the network with privileged access to internal systems.

   - *Application* – Assesses vulnerabilities in the code of a hosted application.

3. **Penetration Test –** Attempts to duplicate the actions of an attacker with the goal of finding paths or weaknesses an attacker could use to access the network.

Ultimately, all three of these assessment options help answer the same question: "Can my network be hacked?" What they don't answer is whether an adversary has used an identified weakness or vulnerability to gain unauthorized access to the network. According to research by Secunia, over 15,000 vulnerabilities are released every year – roughly 25 of which are identified as zero day vulnerabilities (i.e. vulnerabilities that were exploited by hackers before disclosure).[2] With so many vulnerabilities, it's safe to assume that our networks will always carry a degree of vulnerability to hacks – even if fully patched. Worse, an alarming number of breaches which result from these vulnerabilities go undetected for long periods of time.

"IT organizations lack the ability to detect issues and spot early warning signs that malware has slipped past preventive measures."

- Gartner

The Breach Detection Gap

According to research by the incident response company Mandiant, the median time to discover a breach after one has occurred is 205 days. This problem is commonly referred to as the "breach detection gap" (BDG) and is defined as the time elapsed between the initial breach of a network by an attacker and the discovery of that breach by the victim.

Recent network attacks reported by the media continue to highlight the growth of this gap by illustrating various breaches that have gone undetected for weeks, months and sometimes years as the art of security monitoring is unable to keep up with an increasingly sophisticated and pervasive threat. Multiple industry reports state at least 69% of intrusions are not discovered by an internal security process or tool but rather by investigative journalists, law enforcement notifications, or financial fraud monitoring.[3] This takes breach response out of the hands of the organization and puts them into crisis reaction mode.

---

[2] Secunia Vulnerability Review 2016

[3] Mandiant M-Trends 2016, Verizon Data Breach Report 2016

There are many motives for attackers trying to maintain stealthy long term access to a network like this. We call these types of attacks "persistent compromises". Whereas loud attacks like crypto-locker, web defacement, denial of service, or smash and grabs can be easy to identify due to the immediate effect they have, persistent threats meet their objectives by maintaining stealthy long term access to the network.

A common misunderstanding in the security industry is the speed at which an attacker can reach their objectives. Access may be obtained within seconds or minutes depending on the vulnerability exploited, but mapping and navigating a large or complicated network to find the data or individuals the attacker is looking for can, many times, take days or weeks. Additionally, monitoring users on a newly compromised network for a period of time to learn internal operations is essential to an attacker's success as was demonstrated in the Sony attack. Stealing swiped credit cards or monitoring an opposing organization for competitive data gains more value the longer the attacker remains hidden. This however also gives defenders an opportunity to disrupt and counter.

The Compromise Assessment

Over the years, compromise assessments only existed in limited forms as specialized services rendered by boutique incident response firms. As of 2015, the practice has rapidly grown as publically disclosed breaches reached a fevered pitch. Unfortunately, the methodologies, approaches, and effectiveness of these offerings vary widely as standardization does not yet exist.

The first step toward this goal though is to first define the assessment, the goals, and objectives so we may understand how to best accomplish it and what the minimum requirements would be.

We define the Compromise Assessment as:

> An objective survey of a network and its' devices to discover unknown security breaches, malware, and signs of unauthorized access. More specifically, the assessment seeks to find attackers who are currently in the environment or that have been active in the recent past.

To be widely applicable, the assessment should be:

Effective – At detecting all known variants of malware, remote access tools, and indications of unauthorized access. Advanced offerings and solutions should have the ability to go deeper in detection of unknown (zero day) malware variants as well.

Table 1:
Breach Detection Gap Examples

Victim	Reported	Time to Discovery
Michaels Stores	Jan 2014	8 Months
Home Depot	Sept 2014	5 months
PF Chang's	July 2014	11 months[4]
Sony	Nov 2014	~1 Year
Office of Personnel Management (OPM)	June 2015	~1 Year
Trump Hotels	Sept 2015	~1 Year
Undisclosed Mandiant client	2015	8.5 years

Table 2:
Persistent vs Non-persistent Compromises

Persistent Compromises	Transient Compromises
Spying	Extortion (i.e. Crypto-Locker)
Corporate Espionage	Web Defacement
Credit Card Theft	"Smash and Grab" Theft
Botnet Operations	Denial of Service
False Flag Attacks & Pivots	Destructive Worms
Posturing for Future Attack (i.e. military)	

[4] http://krebsonsecurity.com/2014/06/p-f-changs-breach-likely-began-in-sept-2013

Fast – Assess a large network within hours/days.

Affordable – The average organization should be able to conduct it proactively and regularly (i.e. monthly/quarterly).

Independent – The assessment does not rely on existing security tools.

Any assessment methodology selected should deliver on these requirements and should seek to optimize time, cost, and effectiveness. It should be efficient and affordable enough to run at least once a month for the average sized organization. Additionally, the effectiveness of the assessment should not vary significantly with different security stacks, monitoring and logging practices, or network topologies. Independence enables the assessment to be equally useful to a regional business with only basic protections like a firewall and antivirus or a sophisticated global institution equipped with their own Security Operations Center.

Ultimately, the goal of the assessment is to rapidly identify adversarial activity or malicious logic -- not to perform a complete forensic examination. Once the assessment is complete, recommendations should be made regarding proper response and collected evidence should be packaged for the organization to allow them to conduct investigation into root cause or actors behind the attack.

Why a Compromise Assessment?

The role of intrusion detection is typically fulfilled by real-time intrusion detection systems and anti-virus software in conjunction with a continuous monitoring strategy. A compromise assessment differs from intrusion detection in that it is an active dedication of analytical resources with a focus on indicators of successful compromise. For the period of the assessment, there is more time and a wider authority to dig deeper than what is expected day-to-day in real-time monitoring. Additionally, the assessment brings to bare tools and techniques, typically reserved for incident response, that are better suited for detecting post-compromise activity. Compromise assessments are the most effective defense in depth measure an organization can use to ensure no threats make it past their defenses.

Many organizations, especially those in thin margin industries, have yet to define a sufficiently viable investment level for security. These organizations do what is recommended to meet compliance regulations and then accept or shift remaining risk to an insurance policy. For these organizations, a regular assessment should be incorporated into their respective risk mitigation strategies to ensure their environment is not compromised by attacks that are more sophisticated than what the organization can detect at their current level of investment.

Additionally, many organizations have difficulty justifying an increase in their security posture when a breach has not been experienced before. The resulting “catch 22” renders breach detection unlikely due to a continuing weak security posture. An independent compromise assessment can uncover compromises that may have gone undetected, thereby providing the evidence needed to justify additional security investments.

In some cases and industries, a regular compromise assessment may be a viable risk management alternative when continuous monitoring is cost prohibitive or unnecessary.

Use Cases

MERGERS AND ACQUISITIONS (M&A)

Prior to an M&A transaction, the compromise assessment serves as the pre-existing conditions check to ensure the buyer is not accepting the risk and costs associated with an existing compromise. When feasible, the assessment should be conducted during due diligence.

CYBER/BREACH INSURANCE

As Cyber or Data Breach insurance involves an unknown risk of existing compromise, underwriters would be prudent to require a compromise assessment prior to issuing a policy. The resulting report can be used in actuarial decision making alongside vulnerability or compliance reports. Additionally, the assessment may be used annually as a third party audit to ensure the insured is making necessary efforts to detect and report security breaches.

THIRD PARTY & VENDOR RISK MANAGEMENT

Organizations take on a significant risk when bringing on vendors and partners where sensitive data, intellectual property, or customer data is shared. In many cases, a recent compromise assessment report should be requested to ensure the integrity and confidentiality of the vendor’s information networks.

SECURITY PROGRAM VALIDATION / AUDIT

The compromise assessment serves to validate the effectiveness of current security controls and catch threats that may have been missed in the 24/7 cycle of continuous monitoring.

Post-Compromise Detection

Since the compromise assessment focuses on identifying ongoing or successful compromises, the tools and techniques must be able to identify post-compromise activity, dormant and hidden malware, malicious use of credentials, and Command and Control (C2) traffic. This differs from traditional real-time detection solutions which focus on early detection of attacks, exploits, malware installation events which attempt to prevent an attack from succeeding or catching an attack early enough to reduce damage during a breach.

Multiple industry reports state at least 69% of intrusions are not discovered by an internal security process or tool but rather by investigative journalists, law enforcement notifications, or financial fraud monitoring.[3]

Some approaches to hunt and breach discovery in use today are:

- **Anomaly Detection & Analytics** on existing logs, connection, and event data to catch what the analysts might have missed. Unfortunately, this requires sufficient and correct logs/data to be available.
- **Monitor the network** with new/different security sensors (i.e. passive DNS monitoring).
- **Actively scan devices** for indications of compromise (i.e. IoCs, multiple AV engines, artifacts & malicious behavior) using an endpoint-focused hunt solution.

While each technique has the ability to find threats, the first two suffer when used in a compromise assessment. For instance, anomaly detection has the requirement of a known-good baseline to start from. Analytics solutions aren't independent as they use the existing security stack for its' data, which may or may not be sufficient or go back far enough. Monitoring with different sensors can be cost prohibitive or give overlapping coverage with existing sensors presenting no additional value. Additionally, real-time sensors require a period of monitoring which extends the engagement out to 30+ days. After years of hunting using all of these solutions, Infocyte has found that independent scans of endpoint devices using a concept called Full Device Validation is the most effective approach to a compromise assessment.

The Infocyte Solution

By applying Infocyte's hunt methodology to the compromise assessment, Infocyte has demonstrated an ability to perform a compromise assessment that meets all the above mentioned requirements.

Infocyte uses an endpoint validation strategy which scans each device (workstation, server, and endpoint device) on the network. The scan validates everything running on them, what may be triggered to run (via an autostart or persistence mechanism), and also analyzes each system's volatile memory to discover signs of manipulation or hidden processes. The scan is agentless, meaning it does not require software to be pre-installed on systems it is scanning, and is completely independent of the network's existing security infrastructure.

Infocyte's methodology combines agentless endpoint data collection with industry leading threat intelligence, multiple third party anti-malware engines, and proprietary advanced analysis algorithms that enable zero-day and unknowns analysis and detection.

Compromise Assessment services leveraging the automation of Infocyte's patent-pending hunt platform achieve an order of magnitude improvement to speed, effectiveness and simplicity. In many cases, assessments can be completed nearly

six (6) times faster than what is typically required to deploy and use traditional security monitoring and incident response solutions. The goal being to be able to deliver the assessment in the same time as a comparably scoped vulnerability assessment (i.e. a few hours to a few days depending on network size/complexity).

Conclusion

Our networks will always have a degree of vulnerability, organizations struggle to prevent determined attackers out of their networks, and the skilled attackers are remaining hidden for months, sometimes years, before being discovered. Unless we can measure the current state of compromise, we will have an incomplete picture of information risk.

Organizations should look to include regular compromise assessments as part of their overall information and IT risk management strategy. Additionally, organizations should consider employing these same hunt methodologies into security operations as a defense in depth measure. This will enable operations teams to catch what prevention and monitoring technologies miss, and mitigate the possible damage that can be caused from persistent compromises before they are able to execute on their objectives.

Infocyte's hunt platform paired with our in-depth compromise assessment offers organizations an in depth, yet cost-effective, solution to reducing the breach detection gap and ensuring the confidentiality of an organization's networks.

Contact us for more information or read our technical white paper on the Compromise Assessment to learn more about this service: www.infocyte.com

ABOUT INFOCYTE

Developed by former US Air Force cybersecurity officers, Infocyte's hunt technology fills a void left by today's real-time detection solutions. By focusing on the post-compromise activity of persistent attackers and insider threats, Infocyte's unique approach to security helps organizations defend their networks and critical information.

CORPORATE HEADQUARTERS

110 E. Houston St. Floor 7

San Antonio, TX 78205

+ 1.844.INFOCYTE (844.463.6298)

sales@infocyte.com

www.infocyte.com

@InfocyteInc