



Breach Detection: What you need to know.

Detection and Stopping Advanced Attacks

Table Of Contents

- From Computer Games to War Games 3
- Digital Data: The New Competitive Advantage 4
- Warp Speed of Attack. 6
- Targeting 7
- Penetration via Endpoints 8
- Reconnaissance 9
- Paths of Attack. 10
- Exfiltration. 11
- Persistence, Cleanup and Cover-up 12
- Conventional Defenses are too Slow 13
- Detection must be Automatic 14
- Stopping Malware from Executing 15
- Bit9's Advanced Threat Indicators 15

Introduction

Today's cyber attacks have changed in sophistication, in focus, and in their potential impact on your business.

This eBook will outline the tactics today's advanced attackers are using to break into your organization and why you require a defense-in-depth cybersecurity program that incorporates automatic detection and incident response.

The goal of this ebook is to leave you with the knowledge you need to effectively protect your business against today's advanced attacks.

Who should read this ebook?

- + CISO/IT Prepare a business case for effective security solutions
- + CFO Understand the financial implications posed by advanced threats
- + CXO Answer the concerns of your board and stockholders

From Computer Games to War Games

Hacking used to be a game: an opportunity for the most clever and ambitious in the tech community to show off their skills and superiority — this was especially true within the hacking community.

	1990's	2000'S	TODAY
ACCESS	Overt (Showing off)		Stealthy
MOTIVE	Vandalism		Profit, Espionage and/or Damage
METHODS	One Stage/Component Indiscriminate, Mass Distribution Common Vulnerability		Targeted Multi-faceted, Persistent Zero Day
EXAMPLES	1998: CIH 1999: Melissa	2000: ILOVEYOU 2001: Code Red 2003: SQL Slammer, Blaster, Sobig.F 2004: Bagle, MyDoom, Sasser 2006: Nyxem 2007: Zeus	2010: Stuxnet 2011: SpyEye 2012: Gauss 2012: Flame 2013: CryptoLocker 2013: Heartbleed 2014: Backoff 2014: Shellshock

Perhaps one of the best examples of this “old-school” hacker mentality is Kevin Mitnick, who for nearly two decades used social engineering tactics to rack up a collection of “trophies” ranging from pranking McDonald’s drive-thru windows to stealing the source codes to some of the world’s most important technological innovations, including DEC’s VMS and Sun’s Solaris operating systems, before finally being arrested in 1995.

“Today, Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business.”

- *Kevin Mitnick*

Motivated by the challenge, not profit, hackers like Mitnick served more as nuisances to corporations and government agency security teams, than the economic and national security threats they were often portrayed to represent.

Today however, the game has changed. Today’s “hackers” are not the avant-garde lone wolf technology enthusiasts of the 80’s and 90’s but highly organized professional cyber-criminal organizations motivated by greed and nation-state actors with strategic political, military and economic objectives.

Unlike Mitnick, who only communicated with a few close friends, today’s advanced attackers are organized, coordinated professionals operating inside some of the world’s most well financed organizations. Single attack groups can be made up of hundreds, even thousands, of professional hackers who will work together to compromise targeted organizations, industries, or national governments.

Perhaps the most well known example of this new institutionalized cybercriminal is PLA Unit 61398, which operates out of the 2nd Bureau of China's People Liberation Army General Staff Department's Third Department. According to Reuters, this secret cyber espionage unit "is staffed by perhaps thousands of people proficient in English as well as computer programming and network operations" and CNN counts the likes of Coca-Cola, Lockheed Martin, Telvent, US Steel, Alcoa and EMC Security Division RSA among the units victims.

In short, hacking is no longer a game, it's a weapon in a sophisticated and growing underground war for information, money, and power and the impact to businesses and organizations caught in the cross-fire can be enormous.

"A cyberattack could stop our society in its tracks"

- Gen. Martin Dempsey, Chairman of the Joint Chiefs of Staff

Digital Data: The New Competitive Advantage

Every enterprise has high-value information vital to its success. As cyber-attack techniques become more sophisticated, this data is increasingly vulnerable and increasingly in-demand.

In a digital world, data is your most important asset. IBM calls data the world's "next natural resource" and if spending is any indication of importance, it would seem they are right. Spending on IT is expected to exceed \$3.7 trillion in 2014*. Winners in tomorrow's economy will not only harness data, they will protect it.

Yet despite increased IT spending for security, today's organizations appear to be doing a very poor job of protecting data. A recent study by the Ponemon Institute found that the average cost of a data breach to be \$5.9 million per year, a 15% increase over the prior year, with costs ranging from \$680,000 to \$23.1 million.*

When thinking about the potential impact of cybercrime on your business, it is important to remember that the cost of cybercrime includes far more than the value of the stolen information. It includes the costs of business disruption, lost opportunity, legal fees, reporting costs, damage to brand reputation, and recovery efforts.

A 2014 study found that as many as twenty nine percent of customers discontinue their relationship with a company after a data breach.* Imagine if 29% of your customer base dried up overnight. How would you cope?

It is not only the primary owner of the information and customers who are vulnerable — so are networked business associates and partners who represent additional attack surfaces and are often secondary victims of advanced attacks. Perhaps the most well known example of networked businesses and partners being impacted by a data breach is Target, whose \$148 million breach was the result of a targeted secondary attack after their HVAC vendor's system was compromised.

THE HIGH COST OF CYBERCRIME

- + A national retailer lost more than \$2.5 billion in shareholder value after news broke that payment card data from 2,000 of the company's stores may have been compromised.
- + A Fortune 100 CEO was fired and the firm estimates losses, associated with their 2013 data breach, to be at least \$148 million.
- + A competing manufacturer stole source code from a control-system supplier — the supplier's stock dropped 83%.
- + A metallurgical company lost to cyber- espionage technology built over 20 years at a cost of \$1 billion.
- + The Canadian government stopped a \$38.6 billion takeover bid when attacks compromised sensitive information at government agencies and law firms.
- + Civil penalties for ePHI breaches can be up to \$250,000, with repeat/uncorrected violations reaching \$1.5 million per violation, per year.

INDUSTRY SAMPLES	TYPES OF HIGH-VALUE INFORMATION FOR SALES	BUSINESS ASSOCIATES
Healthcare	Patient health information	Pharmacies, insurers
Technology	Intellectual property, trade secrets, patents, designs	Law firms
Government	State secrets, Social Security information	Contractors
Retail	Customer data: personal and financial	Banks
All	Corporate data: contracts, business plans, staff data	Business process service providers

Warp Speed of Attack

Advanced attacks typically are not “smash-and-grab” events. Advanced Persistent Threats (APTs) involve stealthy infiltration of endpoints and ongoing theft of your critical data over time.

GONE IN 15 MINUTES

A cybercriminal group may take months to identify key targets, develop specialized malware to exploit specific vulnerabilities, and exercise remote command and control during the attack.

Most advanced attacks succeed, with more than half resulting in stolen confidential or sensitive data. Experts estimate that the average organization suffers 9 such attacks a year with only around 50% ever being detected, so the odds are you’ve been hacked and you probably don’t even know.

Detection of advanced attacks takes 225 days on average and in most cases is discovered not by the impacted organization but rather third parties such as the FBI, a bank or a credit reporting agency who have noticed unusual network or account activity.

While it may take nearly eight months to detect an advanced attack, once a hacker is in, exfiltration of data can be as fast as 15 minutes.

For those of you keeping score, that’s a 21,000 to 1 time advantage in favor of the hacker.

If one thing is clear, it is that current cyber security defense and detections solutions are not equipped to protect organizations against the explosion in targeted, sophisticated attacks we are seeing today. But why?

The answer is simple. Current signature-based cyber security protection and detection solutions were designed to detect and stop optimistic attacks designed to take over and infect as many computers as possible. They were built in a time when the number of viruses, malware, and attack variants numbered in the hundreds, so blocking only known bad malware made sense.

Stages in an Advanced Attack



The problem is that these solutions can't keep up with the veracity of new malware being created today. AV-Test claims to register more than 400,000 new malware samples a day and most attacks leverage uniquely developed or modified malware hoping to fly under the radar by infecting a single or only a few dozen specific devices, not the hundreds or thousands needed to generate a new signature.

By design, APTs are designed to remain undetected, compromising systems for months or even years. Attackers cover their tracks, trying to erase any evidence of having ever entered the system.

Targeting

Considerable research goes into choosing targets of APTs. Cybercriminals know well the value of credit card information, Personally Identifiable Information (PII), and intellectual property.

GONE PHISHING

Attackers will use social media sites, such as LinkedIn, search engines such as Google, and public sources, such as 10-Ks, S1s, Patent filings, to identify key individuals or devices at targeted organizations or trusted partners who are likely to have access or easy connections to valuable information.

They will use basic scanning tools and other techniques to find if an organization is using exploitable software. Search engines such as Shodan and tools like wifisniffers and Maltego allow attackers to identify connected devices allowing an attacker to identify that a targeted organization is a Microsoft® shop using Windows®-based Office and SQL Server® databases and likely uses Adobe Ready and Oracle Java for business operations. It is not difficult to even know the versions and patch levels of these systems within the organization.

When looking for specific information, the search can often get personal. For example, if targeting a company's finance organization, attackers will often research the company's fiscal calendar year and make educated guesses around when employees are likely to be working on key projects, such as fiscal budgets, to build more convincing spear phishing attacks.

Once this information is gained, attackers will often shift their focus to individual targets. Tracking social media and other digital breadcrumbs to build a profile of an individual's work-schedule, likely projects, education, personal routine, etc which can then be used to execute a targeted spear-phishing attack.

Knowing that their target is likely to open an email with subject lines about budget or headcount, particularly if they use familiar names and titles. Attackers will begin drafting their attack.

Using social media, industry events, and information on the company website, attackers will work hard to embellish the "lure" in this spear-phishing tactic to build a message that appears familiar and relevant to their target. In some extremely sophisticated attacks, attacker may even attend corporate or industry events in which their target participates.

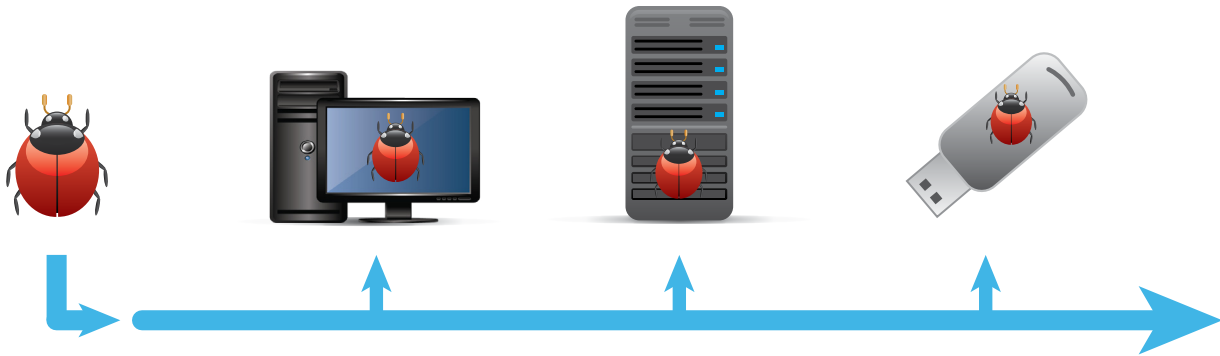
With a tailored subject line and message, the "lure" will contain a malformed document or perhaps a spreadsheet, or it will prompt the recipient to visit a dummy website or to run a program.

If the target doesn't take the initial lure, organized cybercrime or nation-state groups will continue to try him at different times with tweaked subject lines, messages and payload vehicles.

And they won't just target their intended victim — they will also conduct Whois Internet searches for administrative contact phone numbers and emails.

To avoid detection, an attacker might use DNS Lookup for ISP details to make their emails appear more legitimate and to hide their origin. They also switch among multiple network proxies to try and remain anonymous. If the attacker has already compromised a device of a partner elsewhere in the corporate environment, they might even be able to send spear-phishing emails from legitimate corporate or other known accounts.

Penetration via Endpoints



INDIVIDUAL DESKTOP OR LAPTOP

When an attacker is successful and a target opens up the spear-phishing email, he downloads a malformed spread-sheet designed to take advantage of a known, seemingly minor, desktop application vulnerability.

Once the package is delivered to the victims desktop, the attacker can manipulate by remote command and control and look for other "lateral" access points.

One might be a print spooler or driver from which the malware gets administrative permissions.

POS TERMINAL OR SERVER

It's Black Friday, the biggest shopping day of the year.

Updates (particularly of AV with large libraries that drag on systems) are delayed to accommodate the high volume of transactions.

That's the window attackers have been preparing for; they launch an attack that penetrates through known vulnerabilities in older POS terminals and servers and install ram-scraping malware such as "Backoff" or "Rawpos" onto vulnerable POS systems that steals payment information on all credit card transactions during the busy holiday season.

VIA USB STICK

An enterprise has a large mobile workforce, some of whom regularly transfer large amounts of data between co-workers, partners and the home and office.

A file is downloaded from a partners laptop to a USB and, from there, to an employees desktop at work.

Malware moves from the USB onto the desktop (or server) and begins looking for additional vulnerabilities.

Reconnaissance

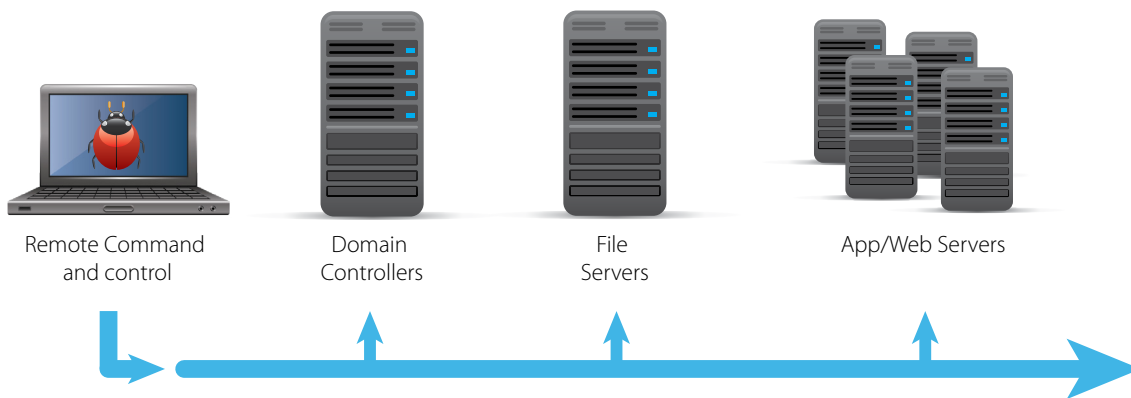
Real-Time Remote Command and Control

“This attack is interactive with a real person sitting at the other end. You can see this in the timing and occasional typos and extra spaces in commands. You can also sense the increase in frustration as the attack progresses — or, rather, fails to progress.

The total attack took close to an hour, after which the attacker probably moved on to a different target. But it is safe to assume that if the compromised system remained in place, the attacker would try again after analyzing this failure.

That’s the very real persistent in advanced persistent threat.”

-Anatomy of a Server Attack. Chris Lord, Systems Architect, Bit9.



Having penetrated an endpoint, APT malware establishes remote command and control so that the attacker can perform stealthy reconnaissance; that is, map the network topology and look for any obstacles and opportunities.

A commonly used tool to map smaller networks or subnets is nmap; a collection of tools (like Paketto Keiretsu) can map larger networks with discovery and network path tracers.

Nmap uses port numbers to show what applications are running on a specific port and can correctly identify many applications by their banners.

The banner also provides version information which allows attackers to identify application vulnerabilities (i.e., outdated patches) that can be exploited to gain further access.

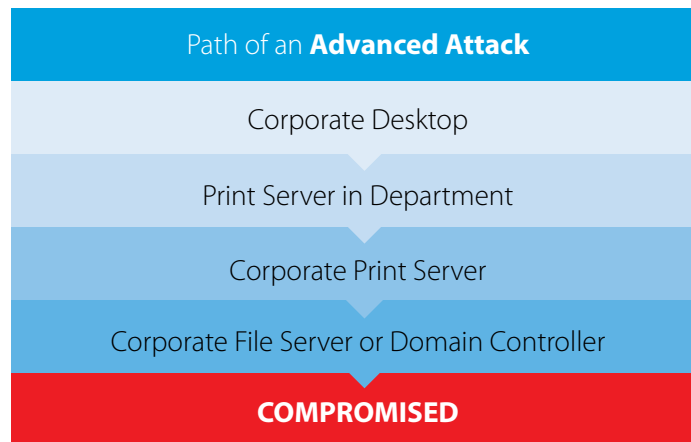
Once the network topology has been mapped and applications identified — including security measures — attackers can use real-time command and control to execute their strategy.

The goal of reconnaissance is to locate servers with the high-value data — and/or to establish routes to administrative credentials that give attackers access to these assets.

Paths of Attack

Having performed their reconnaissance and decided on a route of attack, the real attack begins. From a compromised desktop, an attacker may appropriate local admin rights to gain “legitimate” access to the local print server. With admin permissions on the local print server, it is likely he can advance to a corporate print server or a server located in a department of interest (i.e., finance, development, legal). This route would circumvent firewalls and intrusion detection systems because the communications would appear to be normal print communications. There would be no reason to suspect malware at this point.

Once in the targeted domain, it would be much easier to look for out-of-date system patches, or known vulnerabilities from previous reconnaissance, on file servers or domain controllers. At this point, you have been effectively compromised.



From Digits to Diamonds

THE KEYS TO THE KINGDOM

For attackers taking the long view, domain controllers are a high-value target because they contain the set of passwords and administrative permissions that enable stealthy access on an ongoing basis.

But attackers can also be opportunistic. Having penetrated the system, be it through spear phishing or a zero-day exploit, they will quickly look for unencrypted, high-value databases and file servers containing credit card or PII data, IP and trade secrets. Often this process is automated, through port sweeps and IP filters, helping the attacker scan your network and focus their efforts on devices and connections with known vulnerabilities.



Strategy: Attack Domain Controllers

Steal the “Keys to the Kingdom”: passwords and permissions.

Gives attacker “legitimate” access to resources at will for as long as needed.



Strategy: Attack Databases, File Servers

Especially if data is not encrypted or if attackers spots target of opportunity.

Files/folder names may be revealing: Patents, Source Code, Legal, etc.

Many of the recent high profile Point-of-Sale attacks were compromised with ram-scraping malware after weaknesses in the remote desktop applications, or VNC programs, used by POS maintenance vendors were exploited to allow hackers to take remote control of store systems.

Remote desktop and other service connections are easy entry vectors for hackers because while legitimate, they are often configured by-design by third-party service contractors to allow individuals outside a corporate network to connect and take action on a device. When exploited this can provide hackers with a trusted backdoor into corporate devices from which lateral moves to other devices can then be made.

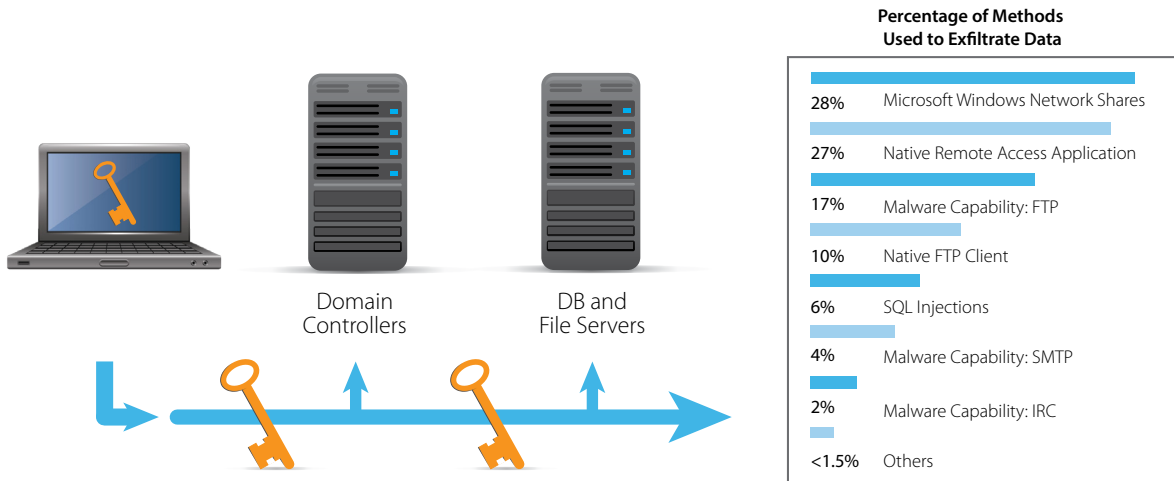
“Restaurant systems had become sophisticated all-in-one solutions that handled everything from order taking to seating arrangements, and they were all based on Microsoft Windows. To support the machines remotely, service vendors were installing them with commercial backdoors, including VNC. With his VNC skeleton key, Max could open many of them at all.”

- Kingpin-How One Hacker Over the Billion Dollar Cyber Crime Underground, 2014.

While unpredictable application exploits are a common attack vector used by hackers, once inside an attacker will almost always require installation of software to complete data collection and begin the exploitation process.

Exfiltration

Attackers decide the time and speed of exfiltration. The most dramatic scenario: downloading an entire database of PII or corporate IP in minutes.



Due to insufficient corporate detection capabilities, APTs often reside on your system for a long time. In 2014, the average attack took more than 220 days before it was detected.

Attacks are well aware of this fact and often take a long game approach to mining for corporate data. Patient, targeted attackers will lurk in the shadows of a corporate network, exfiltrating data slowly to avoid raising alerts.

One technique used to accomplish this is to schedule tasks to run at a later time at a higher permission. They can smuggle out data hidden in packets such that they are very hard to spot — even if you know you were compromised.

As additional data becomes available, attackers will return again and again to access and exfiltrate more data in your environment.

A study of 200 data breaches in 24 different countries showed that the most common method of extracting data is through the same remote access application used for entry. Services such as native FTP and HTTP client functionality were also frequently leveraged for data extraction. When malware was utilized for data extraction, FTP, SMTP and IRC functionality were all observed. (In reverse analysis of custom malware, binaries sometimes disclosed the existence of FTP functionality, including hardcoded IP addresses and credentials.)

Off-the-shelf malware, such as keystroke loggers, most often use built-in FTP and email capabilities to exfiltrate data. When email services were employed, the attackers often brazenly installed a malicious SMTP server directly on the compromised system —to ensure the data was properly routed!

Persistence, Cleanup and Cover-up

Most advanced attacks are not overt, one-time smash-and-grab events. They are designed to persist and remain undetected, even as they communicate back to the command-and-control center for malware updates and modifications.

One tactic is the creation of “dummy” administrative accounts that “fly under the radar” of regular IT monitoring.

Another is leaving behind “back doors” in compromised applications for future access and exfiltration of valuable information.

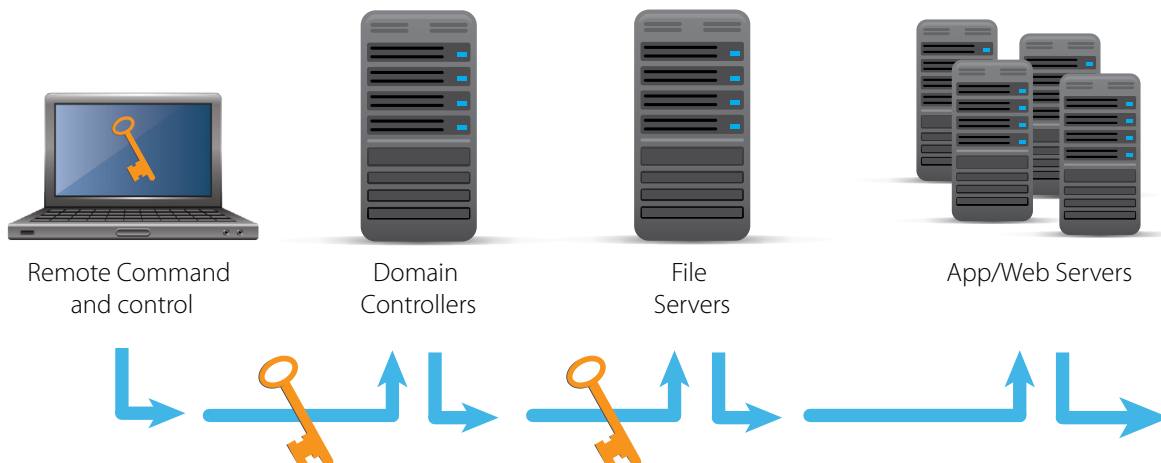
Besides these “crumbs,” the advanced attacker cleans up and erases most traces of itself. The use of forensics to understand an attack and take action to prevent future attacks are challenging.

What’s needed is technology that logs and records all endpoint data in real time so that the crumbs left by attackers can be logged, analyzed, identified and before they are erased and exfiltration has begun.

Some examples of “crumbs” include the information on who wrote a suspicious file, when it was written, where it went on the network, and if it wrote anything else (the spawn of the spawn). This type of information can be extracted — if you know what you are looking for — even if the files themselves have been deleted.

Security technology needs to show you everything that arrived on your system in, say, the last 24 hours or even the last three months. Where was this file, and what was the related activity? It needs to be able to help find and follow the crumbs.

This is key to remediation and, ultimately, prevention.



Conventional Defenses are too Slow

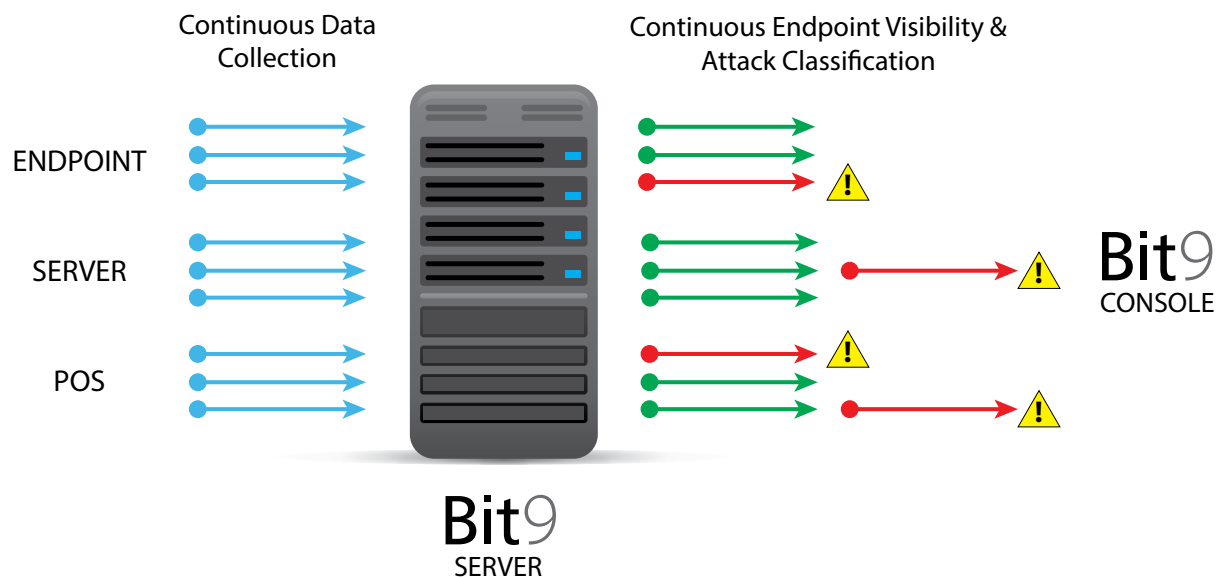
No matter how dedicated and talented, security staff cannot keep up with the volume of data flowing through the enterprise architecture. Security systems like SIEM, IPS/HIPS, and firewalls can in fact add to the data overload.

Quantity of information is one thing, but the real problem for securing your data is the speed with which things happen.

The problem with traditional solutions is they all try to do the same thing: detect and reject malware with a known signature. Next-generation firewalls might be able to alert you that malicious activity is happening but can often do nothing to stop or identify the source of the attack or which devices are impacted. The problem with these solutions is that they look outside your enterprise and try to identify and stop all the malware in the world coming into your enterprise. But that approach isn't sufficient any more, what is required are solutions that combine outside threat intelligence with a strong understanding of your internal environment. Actionable threat intelligence requires more than just understanding what may be attacking your environment, it requires understanding your environment and the relationships inside it well enough to identify bad behavior before it is a problem.

That is why being able to track all executables on your system, whether they run or not, and the relationships between those actions is critical. Without this information you will never be able to reconstruct the elements of an attack and better yet, detect an attack in process.

By changing your focus from the malware you're trying to keep outside your organization to the software you want inside your organization, you can determine what software you trust and only allow that to run in your organization. Everything else, by default, is untrusted and can be automatically denied or flagged as suspicious. This will greatly reduce the attack surface available for hackers to attack your environment.



Detection Must be Automatic

The volume of data and speed of cyber attacks dictate that detection must be automated.

Reactive Tools	Limitations
ANTIVIRUS	Signature based (blacklist libraries); scan based; no sensor to analyze systems in real time
HIPS	Information too shallow: doesn't tell where .exe files were spawned; no historical data for time-based analysis to determine level and impact of potential threat; cannot apply latest indicators to historical data; cannot assess network effect or correlate across all of your systems
LEGACY APPLICATION CONTROL/ WHITELISTING	Relies on combination of AV and HIPS products — and therefore suffers from same limitations as above; can't continuously monitor for suspicious activity; doesn't have the granularity to provide a time-based historical view of each system; no ability to replay an event or attack to understand the threat, risk and impact

Antivirus software, HIPS and conventional application control or whitelisting solutions are based on an after-the-fact, reactive model. Solutions today must be able to reduce your attack surface, provide real-time visibility and incorporate both internal and external threat intelligence to speed up and automate the detection process.

This requires proactive and trust based model which provides rational, automatic filtering to cull and focus the exact information you must interpret.

Stopping Malware from Executing

Automatic detection, embedded in your security environment, is the first barrier to APTs — but suspicious executables need to be stopped until the issue is resolved in order to prevent any damage from being done.

Let's look at a real-world example. With a proactive trust-based model in place, a security team at a banking organization was alerted that a new file had been written by svchost.exe.

Within seconds this file attempted to execute, but because the file hashes were untrustworthy (and not because they were on any AV blacklist — they were not until eight months later), execution was blocked automatically.

Alerts were sent and logged, but at the time there was nothing else to suspect, and no malicious activity had been allowed to occur.

Indeed, it was not until months later when the larger community began to identify components of the complex malware now known as Gauss that the bank realized it had been automatically protected. Gauss was targeting Middle East banks and their users and was successful in compromising many other organizations.


Bit9's Advanced Threat Indicators

The bank that was automatically protected from Gauss is an actual Bit9 customer.

Regardless of your team's incident response experience, Bit9 can provide world-class threat detection by combining real-time sensors, trust-based security, Advanced Threat Indicators (ATIs), and the Bit9 + Carbon Black Threat Intelligence Cloud to automatically detect advanced threats, malware and zero-day attacks that typically evade blacklisting and signature-based detection.

A Bit9 first, ATIs provide security teams with a new endpoint threat detection technology that goes beyond blacklist identification to detect zero-day and sophisticated attacks. A packaged set of rules and views created by Bit9's threat research team that use Bit9's real-time endpoint visibility to identify potentially malicious activities, ATIs leverage patterns and contextual information, rather than single factor binary detection, to deliver fewer, more actionable alerts.

For customers leveraging next-generation network security solutions, such as those from Check Point, FireEye, or Palo Alto Networks, Bit9 can correlate event data from the network to further improve detection, response, and prevention.



	A	B	C	D	E	F	G	H	J	K	L	U	X	Z	AC			
1	Date	Crea	Computer	File Name	Publisher	User Nam	Trust	Threat	Local Stati	Company	Detailed L	Executed	MD5	Prevalenc	Product	Version	SHA-1	SHA-256
2	Aug 10 20:	xxxxxxxxxx	7039273.msi	Microsoft	NT AUTHC			-1 Unknown	Approved	Microsoft	Approved	Yes	51ea1228c	297 5.00.7711.0000			90d52f570 6a3019ae31cc	
3	Jun 25 201	xxxxxxxxxx	client.msi	Microsoft	NT AUTHC			-1 Unknown	Approved	Microsoft	Approved	Yes	51ea1228c	297 5.00.7711.0000			90d52f570 6a3019ae31cc	
4	Jun 11 201	xxxxxxxxxx	winbook.ocx	Microsoft	NT AUTHC			-1 Unknown	Pending	Microsoft	Pending (I	No	8538ff97c	1 05.01.2600.5788			d0322869f 35331bd166d	
5	Apr 30 201	xxxxxxxxxx	lanhlp32.ocx	Microsoft	NT AUTHC			0-2 - Malicic	Banned	Microsoft	Banned by No		ed2b4397f	2 5.1.3700.0			5f4b3de81 0e5bd41d3d0f	
6	Apr 18 201	xxxxxxxxxx	client.msi	Microsoft	NT AUTHC			-1 Unknown	Approved	Microsoft	Approved	Yes	51ea1228c	297 5.00.7711.0000			90d52f570 6a3019ae31cc	
7	Apr 18 201	xxxxxxxxxx	7039261.msi	Microsoft	NT AUTHC			-1 Unknown	Approved	Microsoft	Approved	Yes	a4fc11c02	237 1.2.3520.0			83cea0e8f 4a7c3c38bc68	
8	Apr 18 201	xxxxxxxxxx	7039257.msi	Microsoft	NT AUTHC			10 Unknown	Approved	Microsoft	Approved	Yes	b20bbeb8	238 8.0.61001			3f6508e8 9b8b34b127a1	
9	Apr 18 201	xxxxxxxxxx	703924d.msi	Microsoft	NT AUTHC			10 Unknown	Approved	Microsoft	Approved	Yes	e493a21c5	258 9.0.30729.4148			f57a60104 32c7ccf5d9ac7	
10	Apr 18 201	xxxxxxxxxx	windowsfirewall	Microsoft	NT AUTHC			-1 Unknown	Approved	Microsoft	Approved	No	69123fd2e	297 1.2.3412.0			23d2e6dc: 2039c3ea79b8	
11	Apr 18 201	xxxxxxxxxx	scepinstall.exe	Microsoft	NT AUTHC			-1 Unknown	Approved	Microsoft	Approved	No	9aeb45d5	328 2.2.0903.0			17c90933a 22858f94d449f	
12	Mar 20 20:	xxxxxxxxxx	devwiz.ocx	Microsoft	NT AUTHC			0-2 - Malicic	Banned	Microsoft	Banned by No		cb98203:	2 5.1.2600.0			f801ff5cb1 6a258d85aa76	
13	Mar 19 20:	xxxxxxxxxx	mcdmn.ocx	Microsoft	NT AUTHC			0-2 - Malicic	Banned	Microsoft	Banned by No		9ca4a4913	2 05.01.2600.5788			f60585f9c: fa2d66a93885	

2. Execution Blocked

↓

1. New File Variation

↓ 5th February 2012

↓ Written by svchost.exe

WHY CUSTOMERS NEED BIT9 ADVANCED THREAT DETECTION

If a customer has devices not running Bit9, or if any Bit9 protected systems are not in high enforcement, there is a chance for malware to get in. With ATIs continuously monitoring systems' behaviors, administrators will be aided in their search to continuously monitor their environment by, examining many facets of your system — including files, registries, process and memory execution — to identify potential compromise or infection.

Examples of what ATIs can detect:

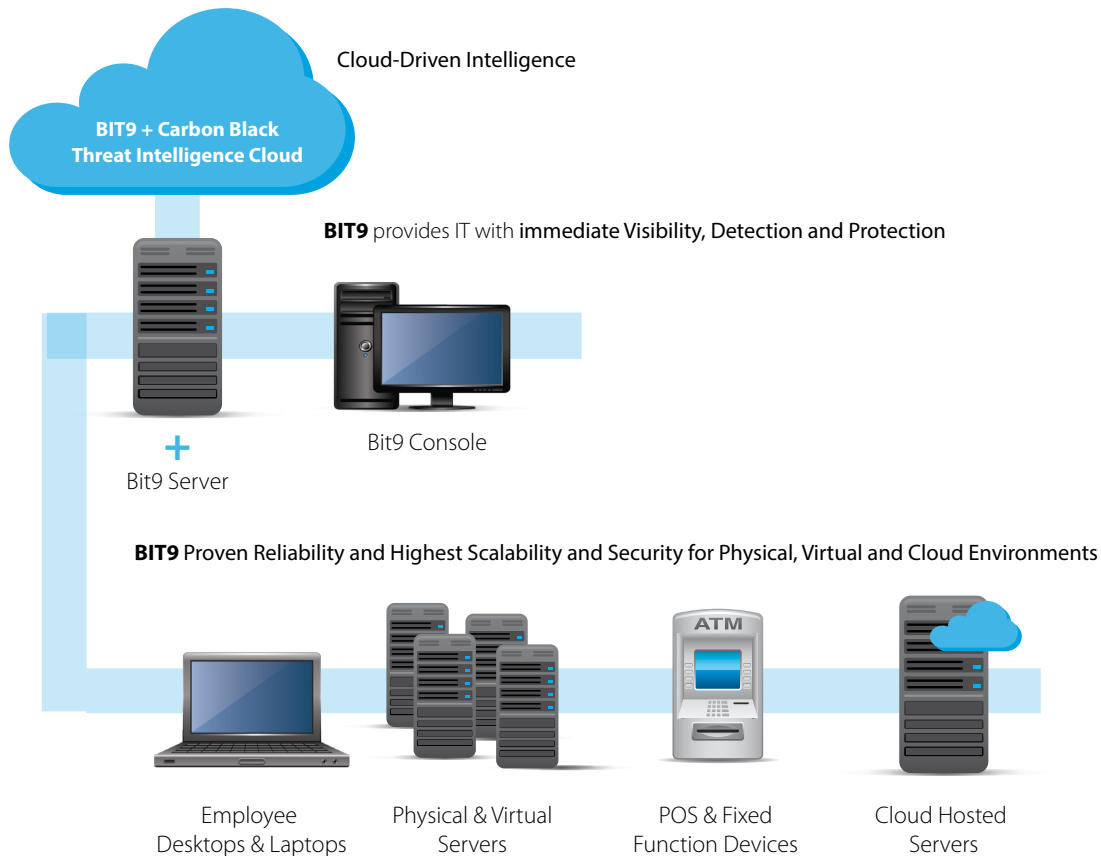
- + A process attempting to harvest cached passwords
- + A PDF file spawning an executable
- + Processes injecting into other processes executing out of suspicious locations

As new threat intelligence is gathered around advanced threats by Bit9's Threat Research Team, your environment is immediately analyzed and your organization automatically alerted to any sign of an attack.

Even with high enforcement, trusted users can knowingly or unknowingly approve malicious files. Bit9's Detection Enhancement provides an additional layer of security.

Bit9 Advanced Threat Detection gives Bit9 customers peace of mind in their ability to not only prevent but rapidly detect and response to attacks throughout their entire infrastructure — servers, desktops, laptops and fixed-function devices.

Get Ahead of Advanced Threats



ABOUT BIT9 + CARBON BLACK

The combination of Bit9 + Carbon Black offers the most complete answer to the newer, more advanced threats and targeted attacks intent on breaching an organization's endpoints. This comprehensive approach makes it easier for organizations to see—and immediately stop—advanced threats. Our solution combines Carbon Black's lightweight endpoint sensor, which can be rapidly deployed with no configuration to deliver "incident response in seconds," and Bit9's industry-leading prevention technologies. Benefits include:

- + Continuous, real-time visibility into what's happening on every computer
- + Real-time threat detection, without relying on signatures
- + Instant response by seeing the full "kill chain" of any attack
- + Protection that is proactive and customizable

Bit9 + Carbon Black delivers a comprehensive solution for continuous endpoint threat security. This is why thousands of organizations worldwide—from 25 Fortune 100 companies to small businesses—use our proven solution. The result is increased security, reduced operational costs and improved compliance.

Bit9 + **CARBON BLACK**

266 Second Avenue
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com