EXPLOIT KITS

GETTING IN BY ANY MEANS NECESSARY

PALO ALTO NETWORKS | 4401 Great America Parkway | Santa Clara, CA 95054
www.paloaltonetworks.com

paloalto NETWORKS®

Executive Summary

Exploit kits are used to automate the exploitation of vulnerabilities on victims' machines, most commonly while users are browsing the web. Exploit kits first became popular in 2006, and since then, their usage has increased dramatically. Because of the automation, an attacker can take an opportunistic approach at scale in going after victims. But at the same time, exploit kits are commonly being used in targeted attacks.

Exploit kits have become an extremely popular method for mass malware or remote access tool (RAT) distribution by criminal groups, essentially lowering the barrier to entry for attackers. To understand this phenomenon, we must understand the ecosystem that surrounds exploit kits, including the actors, campaigns and terminology involved.

For exploit kit creators, there is a massive opportunity to generate profit. Creators can offer exploit kits for rental on underground criminal markets, where the price for leading kits can reach thousands of dollars per month.

Exploit kit campaigns generate a series of events starting with a compromised website that ultimately directs web traffic to an exploit kit. Within the exploit kit, a specific sequence of events occurs for a successful infection. The sequence starts with a landing page, follows with an exploit, and ends in a payload. Ransomware is their most common payload, but exploit kits also distribute other types of malware, like information stealers and banking Trojans.

While exploit kits are highly effective, the situation isn't hopeless. There are measures you can take to protect your organization; for example, reducing the attack surface, blocking known malware and exploits, and quickly identifying and stopping new threats can ensure organizations are not impacted by this pressing threat.

Introduction

Our increasing dependence on networked devices has provided a growing target for criminal activity. As early as the 1970s, commercially available computer systems were known to have serious flaws that could be exploited to gain unauthorized control.[1] With the growth of the internet, malware became a popular method for criminal groups to illegally access or disrupt the operations of an increasing number of connected systems. By the mid-to-late 1990s, most criminals had turned to the internet for malware distribution.[2]

As an increasing amount of valuable data became accessible over the internet, information technology grew more security-focused. Criminal groups were forced to develop sophisticated methods to gain unauthorized access and infect computers. By the 2000s, criminals turned their attention to exploits targeting implementation or design flaws in web-browsing software.

Exploit kits were developed as a way to automatically exploit vulnerable computers browsing the web in a silent manner, simplifying what had previously been a complex process. Starting with the first documented exploit kit case in 2006, other kits quickly followed. By 2010, the Blackhole exploit kit introduced a rent-based business model, and exploit kits continued to evolve. They first relied predominantly on Java® and PDF exploits, in recent years, turning more to exploits for Adobe® Flash® Player and Internet Explorer®. They are currently a widely used and extremely effective method for large-scale malware distribution and profit generation for malicious actors.

Defining Exploit Kits

To understand this phenomenon, we must clearly define what an exploit kit is, and we should also define several terms associated with exploit kit activity.

Vulnerability. This is an unintended flaw in software code that leaves it open to exploitation in the form of unauthorized access or other malicious behavior.

Exploit. An exploit is a file or code that takes advantage of a vulnerability in an application or operating system.

Malware. This is a commonly used contraction of the term "malicious software." If an exploit is successful, it allows a separate malware file to infect the targeted host. In the context of exploit kit activity, this malware is called a "payload." Exploit kit payloads are generally designed to infect hosts running Microsoft® Windows® operating systems.

---

1 https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

2 http://www.tripwire.com/state-of-security/security-awareness/the-evolution-of-malware-part-three-1993-1999/

Exploit kit. An exploit kit (EK) is a server-based framework that uses exploits to take advantage of vulnerabilities in browser-related software applications to infect a client (a Windows desktop or laptop) without the user's knowledge.

Actor. An actor is an individual or criminal group behind a piece of malware. In the context of cybersecurity, the term "actor" is associated with a theater of war. Since good and bad actors exist in any conflict, you will often see the terms "bad actor" or "threat actor" when referring to various criminal groups behind malware.

Campaign. Exploit kits are not effective on their own. Some sort of infrastructure must be established to direct unsuspecting users to the exploit kit. A campaign consists of the exploit kit and the infrastructure used to direct victims to it.

Why Criminals Use Exploit Kits

Exploit kits are attractive to criminals for three main reasons. First, EKs enable a stealthy method of infecting Windows hosts with malware. Second, the exploitation process is automatic. Third, criminals can outsource malware distribution using exploit kits.

Stealthy malware infection. Exploit kits are designed to work behind the scenes during normal web browsing. Hidden code is used to redirect browser traffic to an EK server. This network activity is not visible on the browser.

Automatic exploitation. The EK process is automated. Exploit kits automatically check the person's computer for vulnerable browser-based applications, then they send an appropriate exploit. No hands-on management is required. Once an EK campaign has been established, the criminal can monitor its effectiveness through a control panel.

Outsourcing. Exploit kit use is a convenient method for criminals to outsource their malware distribution. There is no need to build or establish an EK system on your own when it can be rented at a much cheaper cost. Furthermore, you do not require in-depth technical knowledge to use an EK. Equipped with a user-friendly control panel or dashboard, operators can conveniently adjust an exploit kit to fit their need.

Who Uses Exploit Kits?

Generally, exploit kits are used by actors who want to distribute malware on a wide scale. Exploit kit campaigns have a broad reach and can potentially connect to millions of victims. This is a good method to reach as many people as possible.

Actors are generally identified by the malware they distribute. Actors use EKs to distribute botnet malware, information stealers, ransomware, and other types of malware.

On a much smaller scale, exploit kits can be used by criminals for targeted attacks. This is called a "watering hole" attack strategy. In this attack, the threat actor targets a particular organization, region or industry through websites these groups often visit. A website used by the targeted group (known as the "watering hole") is compromised. This compromised website redirects people's computers to an exploit kit. Using this method, a member of the targeted group eventually becomes infected. For example, in 2014, reports surfaced of a watering-hole attack targeting firms in the energy sector.[3]

Criminals have also utilized emails with EKs in targeted attacks. Malicious emails are sent to specific individuals containing links to an exploit kit. This method is not as stealthy as a watering-hole attack, but it can be more precise in its targets.

Exploit Kit Rental

Exploit kits are advertised as for rent to end users at online communities, typically on a daily, weekly or monthly basis. Rates (monthly) range from a few hundred dollars on shared servers to several thousand dollars for a private server (able to quickly process very high rates of infection-candidate traffic). Daily rates in the tens of dollars provide easy EK access on any budget. During the past year, the number of EKs on the criminal market has decreased. We've seen such popular EKs as Angler and Nuclear disappear, and with fewer exploit kits available, a gradual increase in EK prices has occurred. Exploit kits are now, on average, about twice as expensive as they were two years ago. Rates are generally commensurate with the reputation of the (re)seller/service, features, number and timeliness of new exploits, as well as the advertised infection rate. As with other underground markets, reputation is everything.

"Cost: Day / Day - 80 USD Week / Week - 400 USD Month / Month - 800 USD"

"Pricing: Week: 600$ Month: 2000$ Bitcoin only!"

"Аренда на общем сервере с общими чистками:
День — 40$
Неделя — 150$
Месяц — 450$"

Similarly, access to even be able to rent varies – some are open to all on relatively open forums; others are available only on closed, vouched forums – sometimes further limited, for example, to "only Russian" customers (or charging more if not Russian); indeed accepting English-speaking customers is sometimes considered a feature itself.

"We Accept English Speaking Users, You CAN Pay Only Bitcoin"

"especially since [redacted] won't sell me daily and weekly because I'm not Russian"

3 https://www.zscaler.com/blogs/research/lightsout-ek-targets-energy-sector

Some kits are further rented through resellers (with or without permission from the operators).

* - [illegible] - 11-11-2013 08:05 AM

(11-11-2013 07:43 AM) [illegible] Wrote: ▶neutorino is not renting to any other then Russian clients and if he does its 10k a month

yea i know im waiting on swt but i been waiting for a week now still no luck but as far money is not an issue

Nope. He's selling it for $450 a month. I talk to him on jabber every day lol.

> *"I will be leasing spots on neutrino tomorrow. I will be selling*
>
> *1 day = $30 1 week = $100 1 month = $350*
>
> *I will accept: Paypal BTC LTC BTC-E"*

> *"There are 2 known users on this forum selling the exploit kit for $250-$350 per week but in fact they do not have permission to sell from the owner and coder of this exploit kit and they are selling 2 times what it is worth. If you want to buy straight from the owner for the price of $150 per week or $500 per month"*

A small industry also surrounds exploit kits, with some individuals offering assistance with setup services – no matter how much EKs simplify the attack process; this demonstrates that some users lack even the basic technical proficiency to set up the EKs themselves.

The user can source "traffic" (victims for exploitation) themselves or pay third parties to provide a source of infection candidates.

Various factors govern the pricing of EK rental: demand, reputation, support, features and ease of use, exploits, and the regularity of updates/additions.

> *"With This Exploit Kit you get what you pay for, a high quality EK with easy to use panel, many exploits to ensure a high traffic. The clean and modern panel makes using our Ek a superb pleasure with is clean and intuitive interface"*

Exploits:
Spoiler (Click to Hide)
CVE-2016-0034
CVE-2016-1019
CVE-2016-4117
CVE-2016-0189
cve-2015-5122
cve-2015-5119
cve-2015-3043
cve-2015-2419
cve-2015-2445
cve-2015-7645
cve-2015-0311
cve-2014-6332
+ 3 Private Exploits.

Features

#World map
#browser and IP tracking
#GeoLoc available,
#Add & remove Domain on panel
#Add & remove File
#Scan File
#Scan Domain
#Rotator
#Rates 15/30% depends on traffic source.

> *"-Work On all WinOS 32 / 64bi*
>
> *-Bypass UAC on exploits*
>
> *-Fast cleaning + cleaning on request*
>
> *-Keep Large volumes of traffic, no traffic limits*
>
> *-We provide always clean and trust domains with automatic check on the blacklist*
>
> *-We use CVE-2013-7331 for detect and stop AV or virtual machines.*
>
> *-API with automatic delivery"*

"Sample" describes the rate of successful victim infection – a claimed rate of 10 percent is quite typical, up to about 30 percent.

Occasionally, cracked versions are peddled; however, as well as the risk of these (with no small irony) carrying malware to infect the users themselves, they are typically unstable and lack features/updates:

> *"they don't contain the rootkit and are not stable you will loose your bots, none of the plugins and options actually work in those cracked bots and basically are shitt."*

Access to the simplicity of victim infection offered by exploit kits can be easily and quickly obtained even by unsophisticated individuals for a very small amount of money.

How Exploit Kits Work

The authors of most exploit kits use software as a service (SaaS) as their business model. This model is also sometimes called platform as a service (PaaS), malware as a service (MaaS), or exploit kit as a service (EKaaS).

Using the EKaaS model, exploit kits are rented by their creators to threat actors. Kits are made available in criminal markets through advertisements or by word of mouth, where the price for leading exploits is often a few thousand dollars per month. One of the most popular EKs in 2016 was Neutrino, and it was priced at $7,000 a month.[4]

The owner provides the buyer a management console to oversee rented EK servers, but the buyer must provide an attack infrastructure to form a campaign. Infrastructure for a large-scale campaign can likely also be outsourced by criminals who want do distribute their malware.

Once logged into an exploit kit's management console, the main page displays basic statistics and detection status. Another page of the management console can be used to upload a payload (the malware a threat actor wants to distribute). Other pages provide advanced statistics that show, for example, how many antivirus vendors can detect the payload.[5]

4 http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

5 http://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf

Exploit Kit Chain of Events

Within an exploit kit, a series of events must occur for a successful infection. The sequence starts with a landing page, follows with an exploit, and ends in a payload.

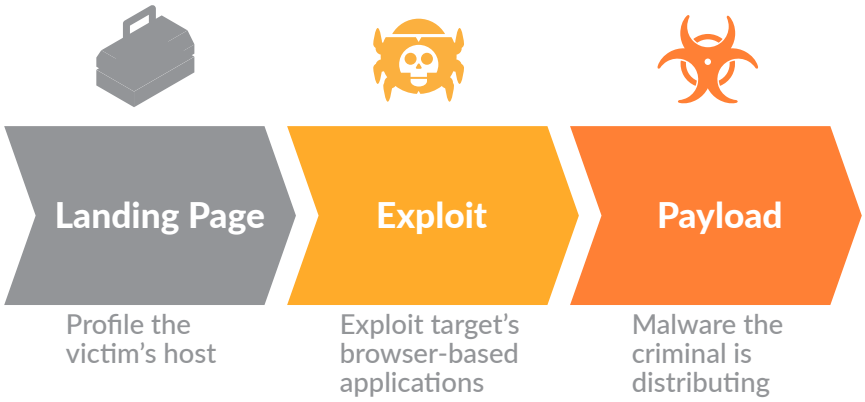

Figure 1 + **Sequence of events for exploit kit activity**

Landing page. The landing page is the first item sent by an exploit kit. In most cases, the landing page consists of code that profiles a victim's Windows computer to find any vulnerable browser-based applications. If your computer is fully patched and up-to-date, EK traffic will stop at the landing page. If not, the exploit kit will send an appropriate exploit.

Exploit. An exploit uses a vulnerable application to secretly run malware on a host. Targeted applications include Adobe Flash Player, Java Runtime Environment, Microsoft Silverlight®, and web browsers (usually Internet Explorer). Exploits allow an attacker to execute arbitrary code on the victim's host. For Flash, Java and Silverlight, the exploit is a file. For vulnerable web browsers, the exploit is sent as code within the web traffic.

Payload. Once an exploit is successful, the exploit kit sends a payload. The payload could be a file downloader that retrieves other malware, or it could be the intended malware. With more advanced EKs, the payload is sent as an encrypted binary over the network. The encrypted binary is then decrypted and executed on the victim's host.

Campaign Chain of Events

As stated earlier, exploits kit cannot infect computers on their own. An EK must have some way of directing users' computers to it. Exploit kits must be part of a campaign.

The majority of campaigns use a compromised website to direct network traffic to an exploit kit. Compromised websites have code injected into their web pages that redirects users to an exploit kit. This provides a straightforward chain of events from the compromised site to the exploit kit.

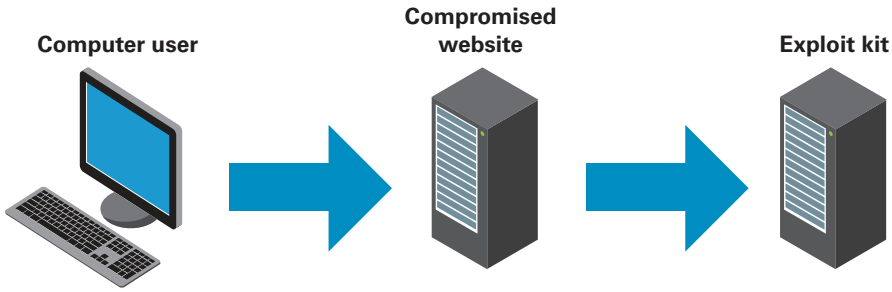

Figure 2 + Sequence of events for a basic exploit kit campaign

Other campaigns use one or more additional servers between the compromised website and the EK server. These additional servers are called gates because they restrict access to the exploit kit. Most often, a gate will only allow Windows hosts to connect with an EK server. If you are using a MacBook® or Linux® host, the gate examines the user-agent string in the web traffic, and it will not forward you to the exploit kit.

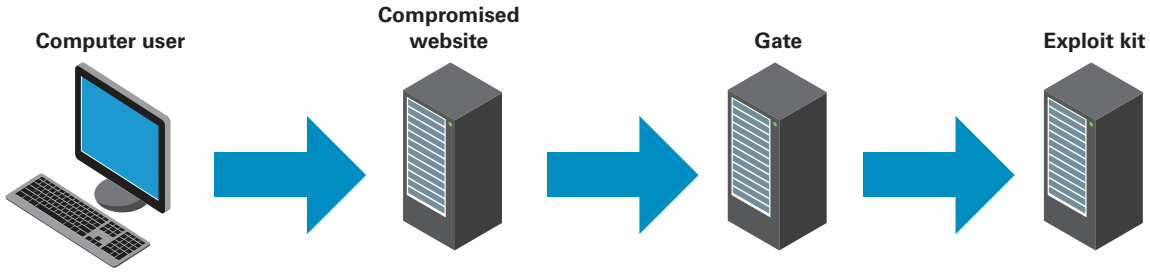

Figure 3 + Sequence of events for an exploit kit campaign using a gate

Malvertising

Malvertising refers to the use of online advertising to spread malware. Exploit kit campaigns can use malicious online ads to reach a large number of potential victims.

Popular websites, like The New York Times or Answers.com, have been used by malvertising campaigns. Those websites were not compromised, but their ad traffic was. Malvertising allows bad actors to fly under the radar and reach an even larger number of potential victims.

Exploit Kit History

Exploit kit activity was first reported in early 2006 with WebAttacker.[6] By 2007, a much-improved EK, called MPack, was marketed, sold and deployed by criminals on a much larger scale.[7] Other exploit kits quickly appeared, like Eleonore and Phoenix.

By 2010, the first version of the Blackhole exploit kit was released. It was the first EK to introduce a rental model for EKaaS. Within a year, Blackhole had grown to become the most notorious and successful of all EKs. Blackhole was generally recognized as the single largest source of web-based exploits by early 2012.[8]

As Blackhole grew in popularity, the number of other exploit kits also increased. At least 20 new exploit kits were identified in 2012 – the largest number of new EKs introduced in a single year.

Exploit Kits Today

The alleged author of the Blackhole exploit kit was arrested in 2013 by Russian authorities,[9] and Blackhole quickly disappeared from the EK scene. Other exploit kits soon filled the void. 2013 had the first recorded appearance of Angler, a kit that grew in sophistication and popularity. Other popular kits include Neutrino and Nuclear (also called "Nuclear Pack"). By late 2014, Angler was the most popular EK,[10] a trend that continued throughout 2015 and the first half of 2016.

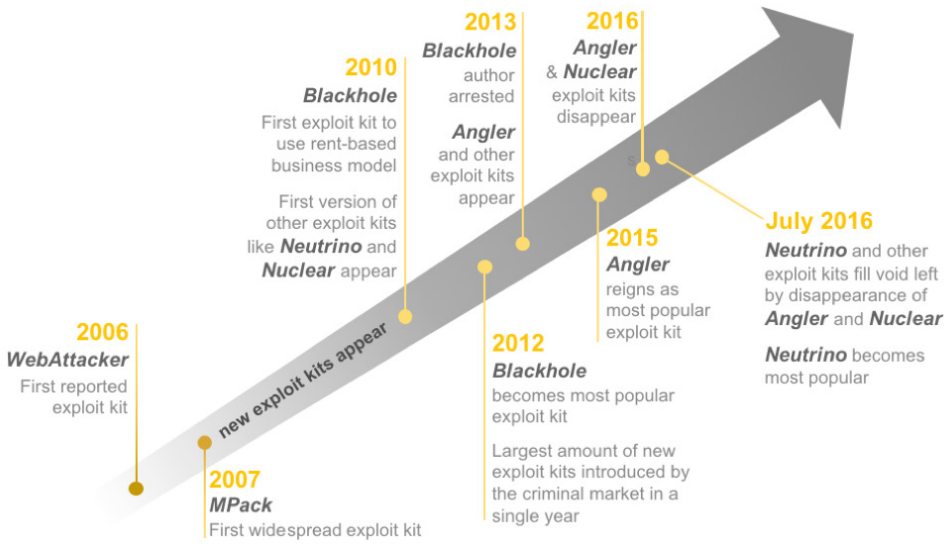

Figure 4 + **A timeline representing exploit kit history**

6 https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

7 http://www.securityfocus.com/news/11476/1

8 https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-14/

9 http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/

10 http://www.securityweek.com/did-angler-exploit-kit-die-russian-lurk-arrests

But the EK scene is constantly evolving. In June 2016, the Angler exploit kit disappeared, an event some suspect is tied to a series of arrests by Russian authorities.[11] By July 2016, the Neutrino exploit kit held the largest share of the EK market.

In previous years, exploit kits relied more on Adobe PDF and Java exploits. In recent years, these kits have turned to exploits for Adobe Flash Player and Internet Explorer.

As operating systems and web browsing applications continue to evolve, EKs will probably turn to other types of exploits. However, despite changing technologies, automated exploitation using web-based exploit kits will likely remain a constant feature of the threat landscape.

Defense Against Exploit Kits

A good defense against exploit kits resembles an effective defense against other types of malware-related attacks. Exploit kits and malware are like guns and bullets, where an exploit kit is the gun, and the malware is a bullet. A defense against EKs should focus on the gun (the delivery mechanism) more than the bullet (the payload).

An organization's response to exploit kit activity depends on the malware delivered after a successful infection. Ransomware is a popular payload delivered though EK campaigns, and an effective response strategy for this type of malware infection has already been covered.[12]

But ransomware is not the only exploit kit payload. Information stealers, banking Trojans, and other types of malware also use this vector of attack. Since EKs are a stealth-based method invisible to potential victims, an effective defense is of utmost importance. Organizations are advised to plan ahead before exploit kits become an issue by employing the approaches that follow.

Attack Surface Reduction

Patch, Update and Upgrade

Since exploit kits target browser-based vulnerabilities, your best defense starts with keeping all applications on your computer fully up to date. Browsers, like Internet Explorer, and applications, like Java and Adobe Flash Player, frequently release patches as new vulnerabilities are discovered. Exploit kit authors use exploits based on the latest vulnerabilities, and they are effective against people who forget to ensure their computers are fully patched. If possible, upgrade to the latest version of Microsoft Windows. The most recent version of Windows has additional security controls that are more effective in preventing infections through EK activity.

11 https://threatpost.com/nuclear-angler-exploit-kit-activity-has-disappeared/118842/

12 https://www.paloaltonetworks.com/content/pan/en_US/resources/research/ransomware-report.html

Limit Usage of Vulnerable Applications

The potential impact of exploit kits can be reduced by limiting access to potentially vulnerable applications, whose risk outweighs the business benefit. This is especially true in the case of Adobe Flash or Java, which are both commonly exploited, and many modern browsers have been moving away from them for some time. Consider controlling access to vulnerability applications for specific user groups, as appropriate.

Access Controls for Network Drives

In many organizations, network drives are connected to multiple systems. If an infected system is connected to a shared drive, all of the files stored on that network drive are at risk, especially if the EK payload is ransomware. This could turn a single infection into an incident affecting users throughout your entire organization. Organizations must implement measures to ensure controlled access to network shares. Network access should always be limited to the smallest number of users or systems possible.

Prevention

Browsing Restrictions

Exploit kits can begin from many different types of websites, with adversaries standing up custom pages, compromising existing sites, or leveraging malicious advertisements through ad networks. Many organizations implement browsing restrictions as a policy measure, but browsing restrictions are also a good way to limit exposure to exploit kits. Security teams should consider web protection that can block traffic to known-malicious domains, phishing sites, or unknown domains.

Network-Based Prevention

Many EKs use a mix of older vulnerability exploits and malware payloads, making it possible to prevent infection by blocking known threats. A combination of intrusion prevention and anti-malware capabilities should be applied at all locations in the network, with the ability to block threats in-line, without human intervention.

Endpoint-Based Prevention

Endpoint protection approaches that have the ability to focus on the core exploitation techniques used by exploit-based attacks are more effective than those that can only focus on individual attacks or their underlying software vulnerabilities. For additional protection, choose endpoint-based solutions that can detect and stop the execution of malicious files delivered by EKs before they start.

Unknown Threat Prevention

Security teams should ensure they have the ability to automatically detect and prevent never-before-seen threats, as attackers evolve their use of exploit kits or change the malware payload delivered by them. Approaches should source new protections from a global network of thousands of organizations, enforcing them in as close to real time as possible.

Data Backup

Since ransomware is a common exploit kit payload, organizations should have a reliable process for backing up and recovering their data. Even if an EK payload is not ransomware, other types of malware put your personal or critical data at risk. An effective backup and recovery plan will decrease the impact of an exploit kit-based infection on your organization. As a best practice, backups should not be accessible to a host with the original data. For example, the data backup should never be stored on either USB-connected hard disks or shared drives on network-accessible hosts.

Testing how you recover files from a backup is just as important as the backup itself. Without periodic testing of your recovery process, you will not identify problems that could prevent you from being able to restore your data after an infection.

unit42

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com