BLUVECTOR®
A COMCAST COMPANY

Ransomware Attacks Are Surging: Threat Report Summary First Half 2021

Contents

For many organizations, the cyber threat landscape in the first half of 2021 can be summarized in a single word: ransomware.

While other types of malware and cyber threats have not gone away this year, the ransomware threat has continued to grow, and massive attacks such as the Colonial Pipeline hack have captured public attention.

This trend shows no signs of stopping, making ransomware protection a critical component of an organization's cybersecurity strategy. In addition, organizations need to be aware of cyberattackers' continued refinement of their techniques and tools and the continued emphasis on social engineering to carry out malicious actions.

Ransomware Attacks Are Surging

In 2020, ransomware attacks surged as cybercriminals took advantage of the effects of the COVID-19 pandemic. This trend shows no signs of abating in 2021. In fact, ransomware attacks have increased since last year, growing by 57%. Additionally, the number of organizations affected per week is greater than in 2020, indicating that this is a sustained trend rather than a sudden spike in attacks.

In addition to being more numerous, attacks in 2021 also tend to have greater impacts. The rise of double extortion attacks — where ransomware gangs steal data and threaten to leak it if ransoms are not paid — has made data breaches a significant concern as well. Some groups are even posing a "triple threat," performing a Distributed Denial of Service (DDoS) attack against an organization to pressure it into paying the ransom.

Ransomware Made Headlines in H1 2021

In H1 2021, ransomware was frequently front-page news. Some of the biggest ransomware attacks of 2021 so far include:

Colonial Pipeline

The DarkSide ransomware group caused a pipeline carrying 45% of the fuel to the US East Coast off-line for a week. The attack prompted the declaration of a national emergency, an Executive Order on Cybersecurity, and the investigation of ransomware attacks as acts of terrorism within the US.

Brenntag

Brenntag is a chemical distribution company and another major victim of the DarkSide ransomware gang in 2021. After the attackers stole sensitive data and encrypted their files, Brenntag paid a $4.4 million ransom.

Acer

In 2021, Acer set records for the largest known ransom demand to date. The REvil ransomware gang demanded $50 million from the company after a ransomware attack and data leak.

JBS Foods

A ransomware attack against JBS foods disabled plants that processed roughly one-fifth of the US meat supply.
The company paid $11 million to the DarkSide ransomware group to restore its operations.

These are only some of the major ransomware attacks that have occurred in 2021 so far, but the news is not all bad. Due to "pressure from the US," the DarkSide ransomware group behind many of these attacks shut down operations in May. Additionally, the US Department of Justice retrieved 63.7 of the 75 Bitcoin that Colonial Pipeline paid to DarkSide.

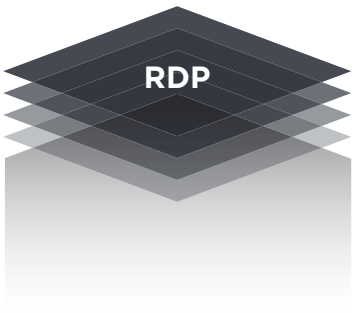
Why Are Ransomware Attacks So Prevalent?

Ransomware attacks surged in 2021 for a few different reasons. One of the biggest is that Ransomware as a Service (RaaS) models became more common among cybercriminals.

Under a RaaS model, one cybercrime group develops ransomware and then distributes it to "affiliates" to use in their attacks. Under this model, relatively unskilled cybercriminals have access to highly sophisticated ransomware, making them much more dangerous than they would be otherwise.

Another major factor in the rise of ransomware in 2020 and 2021 is the COVID-19 pandemic. The sudden shift to remote work forced organizations to deploy infrastructure that is not adequately secured. Ransomware groups have exploited these security weaknesses in their attacks.

The Most Common Ransomware Infection Vectors



The impact of the COVID-19 pandemic has been exemplified by the choice of infection vectors made by many ransomware groups. In the past, phishing attacks were the most common method of delivering ransomware, but exploitation of the Remote Desktop Protocol (RDP) has pushed it into the number two slot. RDP provides a relatively easy way for organizations to support a remote workforce, allowing them to control their on-premise machines over the Internet.

However, the need to expose RDP login portals to the Internet allows attackers to perform credential stuffing attacks or use breached passwords to gain access to employee accounts. With this access, attackers can directly plant and execute their malware where it can do the most damage to the organization.

Behind RDP, phishing is the second most common ransomware infection vector, and exploitation of software vulnerabilities takes the third spot. The risk of unpatched vulnerabilities was made evident by the Microsoft Exchange Server incident, where the release of patches for four critical vulnerabilities inspired the creation of new ransomware variants designed to exploit unpatched systems.

To Pay or Not To Pay?

For ransomware victims, the greatest question is whether or not they should pay the ransom. This question is challenging because there are solid arguments for both options.

From a purely financial standpoint, paying the ransom often makes a great deal of sense. Modern ransomware gangs perform reconnaissance on their targets and align their ransomware demands to what the organization is capable of paying and the value of the encrypted data. In most cases, it is cheaper to pay the ransom than to try to recover from the attack without doing so.

However, this assumes that paying the ransom will actually fix the problem, which is not the case in many attacks. Nearly a third of organizations (29%) that pay the ransom recover only half of their data, and 92% suffer some data loss after paying up.

In other cases, it is actually easier to recover independently than to use an attacker provided decryptor. This was the case for Colonial Pipeline, which paid nearly $5 million in Bitcoin to DarkSide only to find that the decryptor was so slow that they could restore more quickly from existing backups.

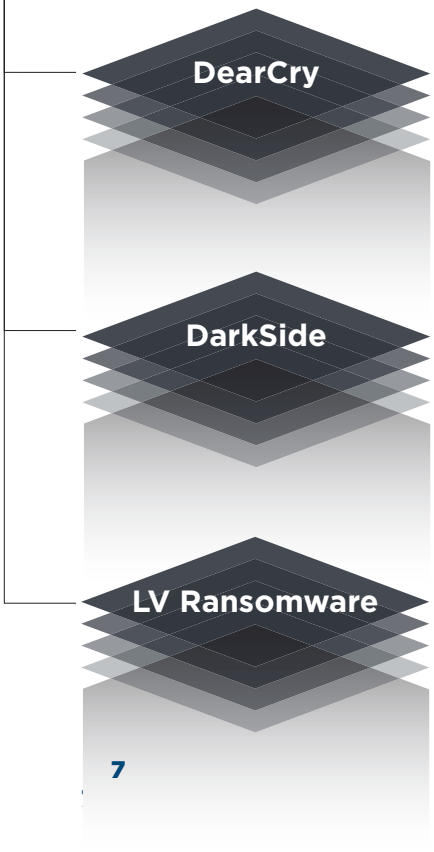
The Threat Landscape in H1 2021

BluVector's insight into customer environments provides both a broad and deep view of the changing cyber threat landscape. There's no question that ransomware has stood out as a significant cybersecurity topic in the first half of 2021.

Other trends reveal that threat actors are using more robust approaches to carry out attacks and that organizations need to become even more diligent about cybersecurity.

New Ransomware Variants Have Emerged

Malware authors are constantly working to improve their code and attack techniques. H1 2021 saw several new ransomware variants.



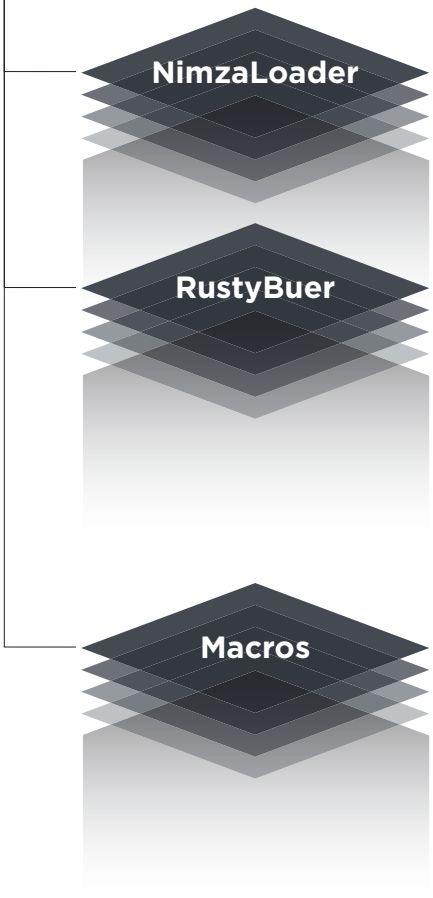
When Microsoft announced patches for several critical vulnerabilities in Exchange Server, cybercriminals rushed to exploit the tens of thousands of potential victims. **As part of this,** the HAFNIUM group created a new ransomware variant **called DearCry.**

Other ransomware groups refined existing malware variants. **DarkSide, famous for the Colonial Pipeline hack,** added the ability to read disk partition information **on an infected computer** and mount additional partitions as needed to encrypt files on them, a feature that was unique among ransomware variants.

In an ironic twist, one new ransomware variant is just REvil repackaged. **LV Ransomware appears to be a pirated version of REvil with a new configuration file.**

Malware Authors Adopt New Programming Languages

Some malware authors have started using less-known programming languages. This makes the malware more difficult to detect and analyze by security tools and reverse engineers.



An early example of this trend is NimzaLoader, which is written in the Nim programming language. To date, **the only other two malware variants written in Nim were created by Zeborcy, a Russian APT.**

RustyBuer is another case **of malware authors switching to a new language.** The Buer Loader was completely rewritten in Rust. The significant effort required indicates that the authors believed that RustyBuer's increased resistance to detection was significant enough to make the switch worthwhile.

More Sophisticated Macros

Microsoft Office macros are a common method of delivering malware. Social engineering is used to convince users to enable macros in a doc, allowing the malicious code inside to run. This attack vector is well-known to security tools, and most documents containing macros are detected and blocked before they reach the user.

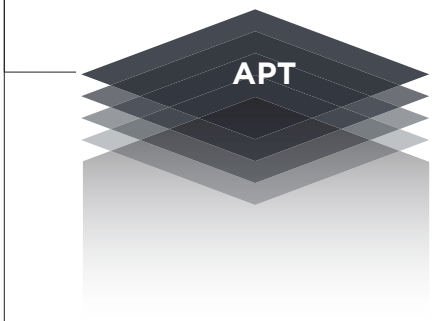
However, recent campaigns have used more sophisticated macros to evade these detections. The Lazarus Group, a North Korean-based APT, developed an innovative technique in which a PNG image is converted to a BMP image, causing a compressed HTML Application file (HTA) with malicious JavaScript to be extracted and executed. The main failure of this technique is that it relies on macros to perform these steps, which increases its probability of detection.

Another recent malware variant of the IcedID trojan uses a completely benign macro. This malware uses content from within the doc (hidden behind an image telling the user to enable

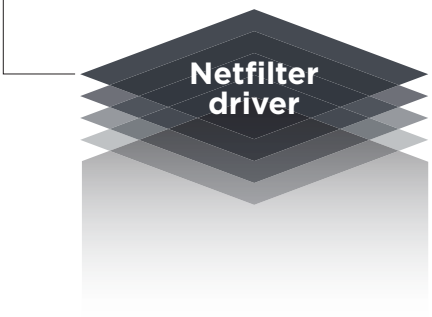
macros) to build a malicious HTA file and execute the malicious JavaScript and VBScript within. The use of a benign macro is designed to evade detection by tools that scan these scripts looking for malicious functionality.

Trust But Verify

The concept of the trojan, where malicious functionality is hidden in a "trusted" file is not a new one. However, in H1 2021, some cyber threat actors introduced variants on the scheme.



The FIN7 APT is known for its deceptive activities, often masquerading as a legitimate cybersecurity company. The group's Lizar backdoor pretends to be an ethical hacking tool for Microsoft Windows environments, but the deception doesn't end with its products. FIN7 is known for posting legitimate-looking jobs with its "security" companies, trying to recruit employees who believe that they are working on legitimate ethical hacking engagements.



Another twist on the trojan is the Netfilter driver, which MIcrosoft accidentally accepted and signed as a legitimate kernel driver. While this malware is only designed to enable cheating at games, its ability to redirect about 350 IP addresses to an IP in China could easily be turned to more nefarious purposes.

Social Engineering Remains Common

Social engineering is a popular technique among cybercriminals because it is simple but effective. Often, tricking a human is easier than evading software-based defenses.

One recent social engineering campaign targets the population most likely to be aware of their techniques: security researchers. The cybercriminals pretend to be legitimate security researchers sharing information about recently-discovered zeroday vulnerabilities. However, the proof of concept code that they provide contains a hidden backdoor.

Another campaign takes the unusual approach of having a phishing email point to a call center. When victims call to cancel their fake streaming subscription, the operator walks them through the cancellation process on a phishing site. Upon pressing the cancel button, an Excel Binary file containing a malicious Excel 4.0 macro is downloaded to the user's computer.

Robust Threat Detection Is Key To Thwarting Cyber Attacks

With several notable cyberattacks making headlines in H121, businesses and the general public alike became more aware of the potential widespread harm of cyberthreats.
Rasomware has emerged as one of the leading issues in the cybersecurity landscape.

With ransomware, hackers can paralyze an organization's operations and extort a significant ransom payment. Funds from ransom payments are akin to venture capital for threat groups, with monies routed into engineering more sophisticated attacks.

The emergence of new programming languages, more sophisticated macros, and the exploitation of trusted assets validate that threat actors are investing in new strategies to evade detection and execute attacks.

Conclusion

Going forward, the prevalence of malware and the emphasis on more sophisticated tools and techniques is likely to continue. To counter these risks, organizations need threat detection and prevention, like BluVector ATD. Taking proactive action to identity threats is a far superior approach to managing the devastating aftereffects of a cyber attack, and every organization needs to take steps to safeguard its infrastructure and operations.

Continued

DearCry: Exchange Server Vulnerability Exploitation With A Side Of Ransomware

A couple of weeks ago, Microsoft released details of critical 0-day vulnerabilities in on-premises deployments of Microsoft Exchange Server, which were being actively exploited in limited and targeted attacks. These initial attacks were attributed to a Chinese based; state sponsored group known as HAFNIUM. Further investigation suggested potentially tens of thousands of victims. According to Microsoft, these targeted attacks enabled access to email accounts hosted by the server and allowed for the installation of malware (including ransomware.) Microsoft urged customers to quickly patch affected systems.

What Is It?

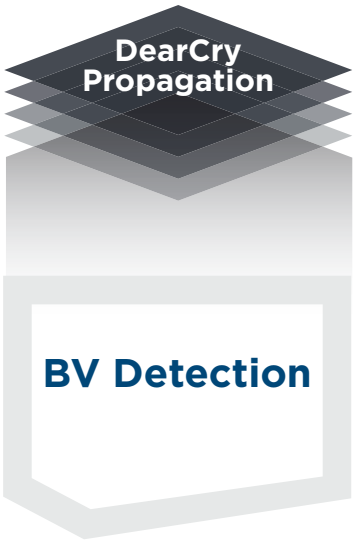
As is usually the case, the technical details of the vulnerabilities and how to exploit them were not publicly released. However, once vulnerabilities are publicly announced and patches made available, both security researchers and attackers compare the vulnerable Exchange Server files with the patched versions and reverse engineer specific ways to exploit the vulnerabilities. This occurs with any high severity vulnerability, however, given the product impacted in this case and the attack surface this provides, the time between when patches are released, and the rush to exploit the vulnerabilities occurs is shortened significantly. This is a primary reason why prompt patching is always imperative.

For some insight into the potential scope of exploitation, despite the fact Microsoft initially referred to limited and targeted attacks, cyber intelligence group Shadowserver have stated that up to 68,500 servers may have been compromised prior to the patches being released. Approximately a week later, Shadowserver found over 64,000 distinct IP addresses were still vulnerable. One of Shadowserver's partner organizations found approximately 20% of the 250,000 servers they scanned were still vulnerable.

Statistics like that would likely make attackers salivate at thought of the profit from the smorgasbord of potential victims to choose from. Therefore, it's no surprise that ransomware operators are making use of the vulnerable systems to deploy ransomware.

One novel piece of ransomware observed using this attack vector is called DEARCRY, also known as DoejoCrypt. Insight from McAfee Cyber Investigations shows DEARCRY victims in Germany, Luxembourg, Indonesia, India, Ireland and the US. The ransomware adds DEARCRY! to the beginning of each encrypted file and uses genuine cryptography, making decryption impossible without payment of the ransom. It also adds .CRYPT to the end of all encrypted files. The attackers provide victims two emails to contact them, with one victim known to have been told to pay a $16,000 ransom.

Once again, attackers have shown a motivation and capability to very quickly make use of new high-profile vulnerabilities to install malware, including ransomware. Vulnerabilities such as these allow ransomware operators to easily and directly install ransomware, without the need for the usually reliable social engineering methods they tend to rely on.



How Does It Propagate?

The malware does not contain the necessary code to self-propagate. The initial attack vector, exploitation of the Microsoft Exchange Server ProxyLogon vulnerability, is discussed in detail above.

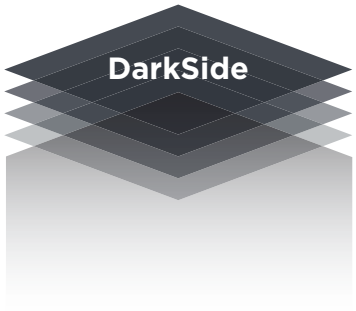
When/How Did BluVector Detect It?

Four samples related to this campaign are publicly available and BluVector's patented Machine Learning Engine (MLE) detected them all. Regression testing has shown the samples would have all been detected 7 months prior to their release.

Continued

DarkSide Ransomware Variant Compromises Disk Partitions

A new DarkSide ransomware variant interrogates the disk drive on an infected system to locate all partitions present, mount additional partitions, and encrypt the files on them. This variant was used in an attack in April 2021. Researchers at found this capability is unique to all currently available ransomware. This example of ransomware-as-a-service (RaaS) shows attackers are adapting and making it easier for less skilled criminals to gain access to novel malware techniques.



What Is It?

Now infamous, due to the Colonial Pipeline attack, DarkSide ransomware was first seen on Russian underground forums in August of 2020; and operates on the ransomware-as-a-service (RaaS) model. RaaS allows other cyber criminals, likely less technically skilled individuals, to subscribe and gain access to ransomware for a fixed percentage of the ransoms paid by victims (usually around 30%). Configuration of the ransomware itself and monitoring of attacks is typically performed through a centralized GUI portal, lowering the technical skill required of subscribers. RaaS operators have borrowed terminology from legitimate Software as a Service and refer to their subscribers as “affiliates.”

Elliptic, a British blockchain analytics company, have reported that since October 2020, DarkSide received a little over $90 Million in bitcoin payments from 47 unique wallets. It appears that owing to the sliding scale of commission the DarkSide developers take, depending on the size of the ransom, that they received $15.5 million, while the affiliates kept a total of $74.7 million.

One of the advantages for affiliates, is access to updated variants of ransomware developed by the RaaS operator. One such new DarkSide variant is described in research recently released by Fortinet. Fortinet found a variant of DarkSide which utilizes a capability they believe to be unique to all currently available ransomware. That being, the ability to read disk partition information and potentially encrypt files, on additional disk partitions, within infected systems. We would like to highlight that this variant was not used in the Colonial Pipeline attack.

This new DarkSide variant interrogates the disk drive on an infected system to locate all the disk partitions present. It skips certain types of reserved system partitions and attempt to mount additional partitions and encrypt files on them; potentially leading to increased impact on multi-boot systems and those containing data partitions. We can assume, the authors believe the effort invested in researching, and coding this feature will, quite literally, pay-off for them.

The sample described by Fortinet was used in a known DarkSide attack against a victim in April 2021. When we executed the sample for analysis in a virtual machine, it was apparent the ransom note was not generic but unique to this specific attack.

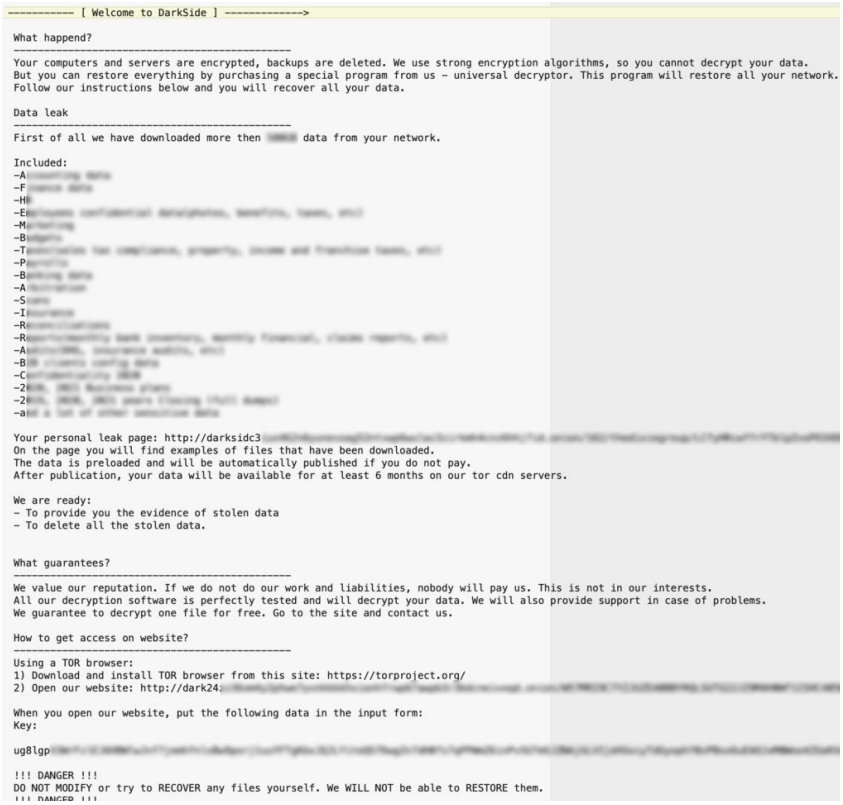
The ransom note lists how much data the attackers claim to have downloaded from the victim's network and details the specifics data downloaded. The attackers offer to provide evidence of exfiltrated data and claim that upon payment of the ransom, all stolen data will be deleted. Exfiltration of sensitive data prior to executing the ransomware is now a common tactic, used by attackers as additional incentive for victims to pay the ransom, or risk having their sensitive data publicly released.

The attackers also guarantee to their victim, their decryption capabilities will decrypt all files – going as far as offering support in the event there are issues on the back-end of the ransom payment being made. DarkSide's intent is to make the entire process of paying the ransom, and decrypting files, as easy as possible. It can be assumed the criminals also want to reduce a victim's motivation to recover files via backups.

The filename for the ransom notes we analyzed contains an eight-character hexadecimal string, "c177efc0", which is also used as the file extension for encrypted files. In the case of RaaS malware, this string is either the affiliate's ID or a unique ID to identify the campaign or specific target.

Continued

Example of a DarkSide ransom note from the April 2021 sample BluVector analyzed.



```
---------- [ Welcome to DarkSide ] ------------->

What happend?
---------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
---------------------------------------------
First of all we have downloaded more then [redacted] data from your network.

Included:
-A[redacted]
-F[redacted]
-H[redacted]
-E[redacted]
-M[redacted]
-B[redacted]
-T[redacted]
-P[redacted]
-B[redacted]
-A[redacted]
-S[redacted]
-I[redacted]
-R[redacted]
-R[redacted]
-A[redacted]
-B[redacted]
-C[redacted]
-2[redacted]
-2[redacted]
-a[redacted]

Your personal leak page: http://darksidc3[redacted]
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.


What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://dark24[redacted]

When you open our website, put the following data in the input form:
Key:

ug8lgp[redacted]

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

How Does DarkSide Propagate?

The malware does not contain the necessary code to self-propagate. However, this DarkSide ransomware variant is capable of encrypting files on alternate disk partitions and network shares. As with most ransomware, initial attack vectors utilized by DarkSide ransomware attacks are often poorly secured internet facing servers, exploitation of unpatched software vulnerabilities and spear phishing emails.

When/How Did BluVector Detect It?

One sample of DarkSide partition encrypting ransomware is publicly available and BluVector's patented Machine Learning Engine (MLE) detected it. Regression testing has shown the sample would have been detected 88 months prior to its release.

Additionally, 27 other recent DarkSide ransomware samples, 24 Windows executables and 3 Linux executables, were also regression tested. All 27 were detected by BluVector's patented Machine Learning Engine (MLE) and would have been detected an average of 75 months prior to their release.

You Can't Trust Anyone - Is LV Ransomware just a pirated version of REvil?

Cyber criminals find opportunities within their own den of thieves. Recent findings published by Secureworks, suggest that REvil is being binary edited and used by LV Ransomware, for their own profit. Yes, malware creators are being exploited by other criminals, who aren't investing resources to create a capability from scratch. LV Ransomware has figured out how to partially reverse engineer REvil's malware, using readily available tools.

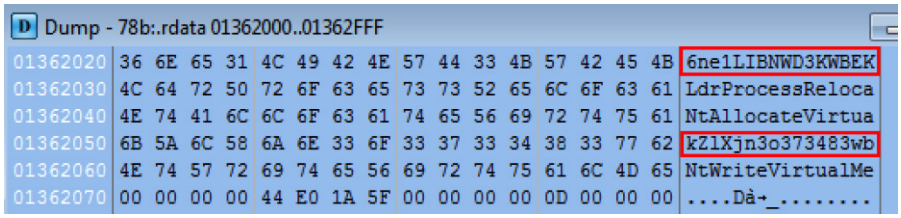
What Is LV Ransomware?

The REvil/Sodinokibi ransomware was first discussed in a Threat Report from May 2019, soon after it was first discovered. It rapidly rose to prominence as a RaaS (Ransomware-as-a-Service) offering, filling the void created by the disappearance of the GandCrab ransomware group. By some accounts, REvil ransomware is responsible for approximately 4 percent of attacks and was one of the first to utilize the tactic of leaking and selling stolen data in an attempt to increase pressure on victims to pay the ransom, a tactic now generally referred to as double extortion. In late 2020, the REvil developers claimed to be profiting to tune of over $US100 million a year, and that's just their share, with the bulk of the profits going to the "affiliates," the customers who utilize REvil for attacks via the RaaS offering.

Based on findings released by researchers from Secureworks, it appears that one of REvil's rivals, LV Ransomware, may just be a pirated copy of REvil. This is a somewhat an ironic situation, of cyber criminals having their malware appropriated by another group without authorization. Adding insult to injury, it appears the theft, may not have been too difficult to achieve. Using some reverse engineering skills and a few simple tools, including a hex editor, the LV Ransomware "authors" have replaced the encrypted configuration file, stored inside the malicious payload, itself stored inside the REvil/LV Ransomware executable. This process did not require any access to, or knowledge of, the REvil source code.

During analysis, the BluVector Threat Team performed the steps, using a publicly available LV Ransomware sample. The first step was to unpack the malicious payload from the LV Ransomware sample. The malicious payload was encrypted and stored in the

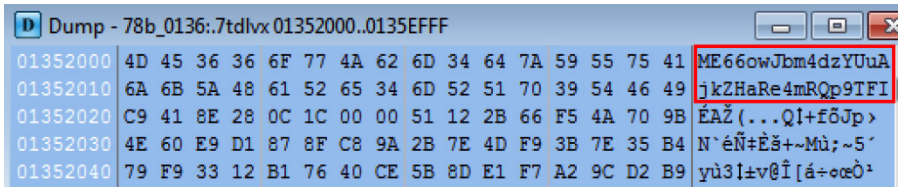
enc section of the sample. The 32 byte key used to decrypt the payload was stored as two separate 16 byte strings in the .rdata section of the sample. The payload can be decrypted using the key and the RC4 algorithm. The payload is the actual LV Ransomware executable.



Data key used to decrypt the payload.

Decrypting the configuration file found in the payload executable is a very similar process. The .7tdlvx section contains the encrypted configuration file; the key:, a hash of the encrypted data; and the length of the configuration data. This time the key is the first 32 bytes of the .7tdlvx section. Once again, using the key and the RC4 algorithm – the configuration file, a JSON formatted text file, can be decoded.

The configuration used by LV Ransomware samples contains an empty dmn entry, in REvil samples this is used to specify Command & Control (C2)sites, potentially indicating LV's authors do not yet have a back end infrastructure mirroring REvil's. This point adds further credence to the theory LV Ransomware is based solely on reverse engineering a REvil sample, with no visibility to other components of the full REvil infrastructure.

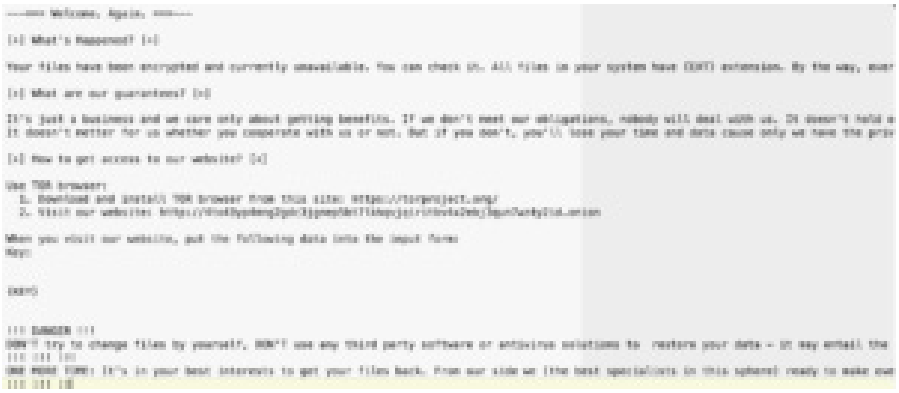


7tdlvx key

Continued

Config file

Once the LV Ransomware author obtained an un-encrypted copy of the configuration file following these steps, they could modify it to meet their needs. The most obvious modification being the ransom note text. Once the configuration file is modified, it's basically the reverse process to create a functioning LV Ransomware sample. First the configuration file is encrypted using a 32 byte key, then the key, encrypted configuration hash, configuration length and the encrypted configuration are put into the .7tdlvx section. This is a process which can be achieved using a hex editor. Then the edited payload executable itself, needs to be re-encrypted, using the key from the .rdata section. It is then placed in the enc section, within a copy of the original sample. This step, once again, can be performed using a hex editor.

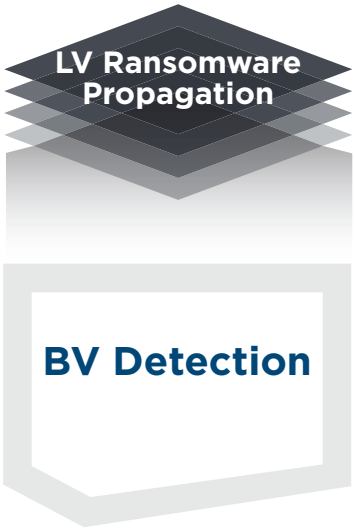


LV Ransom Note

The end result is that the LV Ransomware authors now have a functioning version of REvil ransomware utilizing the configuration file they altered to their needs. As previously stated, all it took was some reverse engineering knowledge and a few tools, mainly a hex editor. However, to paraphrase the words of Dr. Ian Malcolm in the first Jurassic Park movie, perhaps the LV Ransomware authors were too focused on whether they could have done this, rather than spending time considering if they

should have done it. As mentioned, REvil ransomware is a highly lucrative enterprise and it's developers are unlikely to take kindly to individuals, or groups, profiting from their malware. Often large scale cyber criminal operations are backed by, or directly operated by organized crime, which makes "pirating" REvil ransomware a potentially unwise undertaking, to say the least.

Secureworks researchers stated they found no evidence of LV Ransomware being advertised on the usual dark web forums. Knowing this, and the apparent lack of any LV Ransomware back end infrastructure, strongly suggest, it is a lone wolf operation. A lone wolf looking to secure a small portion of ransomware profits for themselves.



How Does It Propagate?

The malware does not contain the necessary code to self-propagate. LV ransomware is known to use spam emails containing malicious attachments as the initial attack vector.

When/How Did BluVector Detect It?

Six samples (including one which was unpacked) are publicly available and BluVector's patented Machine Learning Engine (MLE) detected them all. Regression testing has shown the samples would have been detected for an average of 84.5 months prior to their release.

NimzaLoader uses obscure Nim language to avoid legacy detections

Researchers at Proofpoint recently described an obscure malware named NimzaLoader and Walmart's internal security team recently described similar malware named Nimar Loader

Proofpoint describes the use of NimzaLoader as an initial backdoor, installed onto victim's systems via a highly targeted spear phishing campaign by a group they refer to as TA800, who were previously linked to Bazaloader.

Continued

What Is It?

The concept of security by obscurity is an interesting one. It was once used somewhat derisively, or as an in-joke, by experienced security professionals to describe the security posture of a product or service which uses secrecy rather than other types of controls to secure itself. However, in the increasingly commoditized and profit driven world of cyber-attacks, it can be become a truism. If a product, operating system or platform attracts only a fraction of market share, then from an attacker's point of view it may not make sense, from a return on time and effort basis to attack that entity.

From a defender's point of view, security by obscurity is essentially no security at all and fraught with risk, it is obviously no substitute for actual security measures. However, from an attacker's position, security by obscurity can sometimes be used to their advantage, especially if their goal is to evade detection by legacy signature-based detection tools. These tools require signatures be created and distributed to provide detection of threats, so if a new threat is sufficiently different to existing threats, it will not be detected.

The malware is written in the relatively new and obscure programming language, Nim. Only two other malware variants written in Nim have previously been observed, both from the Russian APT group Zebrocy, also known as APT28, one in April 2019 and one September 2020. In addition to evading signature detections, using an obscure language will also make automated detection by sandboxes and even by human analysts less likely. It also makes reverse engineering of a sample slower and potentially more difficult.

The attack chain begins with phishing emails that use information such as the user's name, organization's name, or both in the body of the email in an attempt to make it appear more credible. The emails contain links which purport to be a downloadable PDF, but actually result in download and execution of the NimzaLoader malware.

Once installed, NimzaLoader contacts it's C2 (command and control) site to receive instructions, it's primary function is to download and execute further malware. It appears NimzaLoader may have been used to execute a Powershell command resulting in a Cobalt Strike beacon being installed. At this time, NimzaLoader's C2 sites are no longer up, and a hardcoded

expiration date has passed, indicating the attackers may still be developing this malware and this campaign was a limited scope test.

How Does It Propagate?

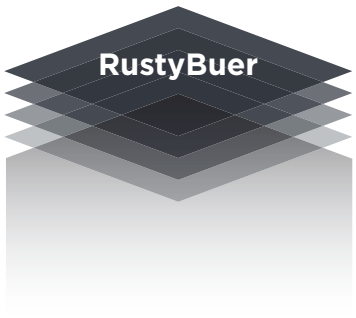
The malware does not contain the necessary code to self-propagate. The initial attack vector is the use of spear phishing emails.

When/How Did BluVector Detect It?

The NimzaLoader sample related to this campaign is publicly available and BluVector's patented Machine Learning Engine (MLE) detected it. Regression testing has shown the sample would have been detected 35 months prior to its release.

If you can't beat 'em, try a new language: New Buer Loader Variant RustyBuer is written in Rust

As a recent Threat Report discussed, attackers are using novel programming languages in an attempt to evade detection. In this earlier case, researchers at Proofpoint found NimzaLoader malware that utilizes Nim, a relatively new and obscure programming language. Recently, they found a new example of attackers attempting to evade detection, using Rust to develop a variant of Buer Loader, RustyBuer.



What Is RustyBuer?

In a new report, Proofpoint researchers have discovered a new variant of the Buer Loader downloader, written in the Rust language, which they have dubbed RustyBuer. Though Rust is significantly more common than Nim, with the first stable version being released in May 2015, it has not often been used to author malware.

Continued

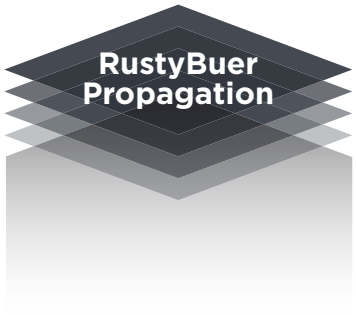
The Buer Loader downloader was first released in late August 2019 and is often used by malware-as-a-service operators to download various trojans and ransomware. Buer was originally written in venerable programming language C. Due to the effort required, it is an uncommon step to see an existing malware variant completely rewritten in another language. We can assume the authors believed the investment in this effort would be rewarded by improved detection evasion, rather than take this as a sign that Rust programming is becoming trendy.

The phishing campaigns delivering RustyBuer began in early April 2021 and were wide ranging, targeting over 200 organizations covering 50 industry verticals. These campaigns mainly used lures relating to DHL parcel deliveries; and included Microsoft Excel or Word documents containing malicious macros which dropped the RustyBuer malware. There were similar campaigns distributing the original C based Buer, however researchers found the social engineering components of the RustyBuer campaigns were more convincing, with an improved likelihood of succeeding. Once executed, RustyBuer uses a Windows shortcut file to ensure it will always be run at startup.

RustyBuer's purpose is to compromise a host, obtain persistence and download additional malicious payloads. In some cases, these campaigns resulted in the downloading of a Cobalt Strike Beacon. As we have mentioned in previous Threat Reports, while Cobalt Strike is a legitimate tool used for penetration testing, it is frequently leveraged by attackers to create a backdoor on an infected system. Interestingly, it was found that some campaigns did not result in an additional payload. This suggests that in some cases, the operators may be using RustyBuer as an access-as-a-service offering, selling their foothold on infected systems to other malicious actors.

If malware authors see improved detection evasion by using new or less common programming languages to write or rewrite new malware variants, we will see this trend continue. Malicious actors will continue to adapt and change, if their efforts deliver value; generating additional revenue. They will continue to employ this tactic, until it becomes necessary to alter their tactics once again.

Continued



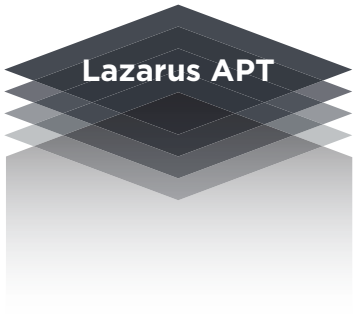
How Does It Propagate?

The malware does not contain the necessary code to self-propagate. The campaigns related to RustyBuer utilized phishing emails with Office document attachments, containing malicious macros, which dropped the RustyBuer malware.

When/How Did BluVector Detect It?

One sample of RustyBuer referenced by Proofpoint's researchers is publicly available and BluVector's patented Machine Learning Engine (MLE) detected it. Regression testing has shown the sample would have been detected 36 months prior to its release

Lazarus APT uses an embedded image to conceal a RAT payload



What Is It?

A malware infection chain is the sequence of events which must occur for a malware payload to be successfully executed on an endpoint. From an attacker's point of view, the object is to evade all detection mechanisms attempting to stop an endpoint becoming compromised and infected. From the defender's perspective, while it is advantageous to be able to detect each step of an infection chain, as long as the infection chain can be disrupted at any point before the execution of the malicious payload on the endpoint, then the threat is mitigated.

A great deal of effort continues to be expended in moving beyond legacy, signature-based detection tools on endpoints and improving detection efficacy. As such, attackers often direct the bulk of their time and energy to evolving techniques to evade endpoint detection. However, sometimes attackers neglect to consider the entire infection chain in their zeal to utilize innovative evasion techniques on the endpoint.

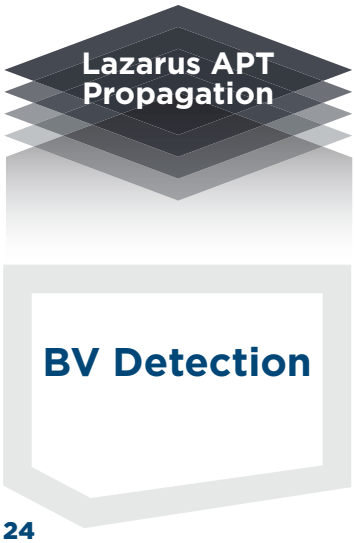
One such example was recently described by researchers from MalwareBytes targeting users in South Korea. They have attributed the campaign to the North Korean Lazarus APT group. The infection chain utilizes a multi-step process to extract, decrypt and execute a malicious payload from a Microsoft Word

document. It includes a novel technique using a JavaScript in a HTA file, embedded in a BMP image, that itself is stored in a PNG image file, to drop the malicious payload. The intention of course being to evade detection on the endpoint.

However, the initial component of the infection chain is a Microsoft Word document containing a malicious macro. This technique is decidedly lacking in innovation and is one which likely has a relatively high probability of detection. (Though at the time of writing, VirusTotal detection for this sample was only 29/60.) This technique also relies on successfully socially engineering the recipient to allow macros to execute, assuming it is not detected before reaching the user's inbox. The document purports to be an application form for participation in a fair in a South Korean city, and the filename translates to "Application form.doc".

If the user permits the macro to execute, it saves the Word document out in HTML format, which also saves all the document's images out as files. It then reads in one of the PNG image files and uses a built-in function to convert it to a BMP image file. The attacker does this because PNG image files are compressed and BMP files are not, and the PNG file contains a compressed HTA fie that is decompressed when the file is saved as a BMP. It is a clever technique to bypass detection of embedded objects on the endpoint. The HTA file is executed, which results in the JavaScript it contains running to create and execute the malicious RAT (Remote Access Trojan) executable.

While utilizing a clever technique to evade detection of the malicious payload on the endpoint, the basic approach of a malicious Word document attached to a phishing email creates a high probability the effort in developing this new technique will be rendered moot by detection higher up in the infection chain.



How Does It Propagate?

The malware does not contain the necessary code to self-propagate. The initial infection vector is a Microsoft Word document containing a malicious macro.

When/How Did BluVector Detect It?

Two samples are publicly available and BluVector's patented Machine Learning Engine (MLE) detected both. The first of these is the malicious Microsoft Word document at the beginning of the infection chain. This sample would have been detected 84 months, or a full 7 years, prior to its release as part of this campaign. The

second sample is the malicious executable, which although it is decrypted and extracted on the endpoint, could potentially be seen if it was copied over the network, possibly by a simple backup. This sample would have been detected 52 months prior to its release, giving an average detection across both files of 68 months.

FIN7 APT Group's Lizar Backdoor Claims To Be An Ethical Hacking Tool

The FIN7 APT group, based in Eastern Europe, is alleged to be responsible for payment card breaches involving well-known brands Chipotle, Chili's, Arby's and Red Robin. FIN7 exploits financial institutions and payment terminals. Specifically, they target restaurants, gambling, and hospitality-oriented entertainment venues. The estimated value of the attacks is $900 million. Researchers believe FIN7 APT group is distributing Lizar malware, claimed to be an ethical hacking tool.

What Is It?

The FIN7 APT has been successful utilizing its Cabana RAT (Remote Access Trojan) to compromise various financial institutions and payment terminals. In April 2021, a senior member of FIN7, a Ukrainian national, was sentenced to 10 years in prison.

FIN7 has previously utilized a front company, Combi Security, to appear reputable. The company allegedly had offices in Moscow and Haifa, Israel; and advertised for penetration testers to recruit for seemingly legitimate roles. One job advertisement on a Ukrainian job board stated that Combi Security had 21-80 employees, and that the company was "one of the leading international companies in the field of information security". It is conceivable that some of the ethical hackers hired by Combi Security believed their roles and their assignments were genuine.

Research published by BI.ZONE suggests that FIN7 have returned to their previous modius operandi, by distributing Lizar. Lizar claims to be a genuine ethical hacking tool for Microsoft Windows networks, but is in-fact the latest evolution of their backdoor. Researchers believe FIN7 is still hiring individuals who are likely not aware the tool is malware; and that they are employed by a cyber-criminal enterprise.

The Lizar backdoor toolkit has been observed in the wild since late February 2021, mainly associated with infected systems across the United States, though victims have also been seen in Germany and Panama. Organizations infected include educational

institutions and pharmaceutical, gambling and finance companies. Lizar is believed to be under active development, and more attacks utilizing this malware are anticipated.

Conceptually, the Lizar backdoor toolkit is similar to Carbanak and uses a modular architecture. The modular approach allows for ease of development and addition of new functionality. The main components are a loader and a series of plugins, which together operate as a malicious bot. The functions of the plugins include loading existing tools such as Mimikatz or Carbanak itself to take screenshots and exfiltrate various sensitive information and credentials. Communication between the backdoor and server is encrypted, the encryption key is specified in the configuration and must match the key on the server, otherwise the communication is ignored.

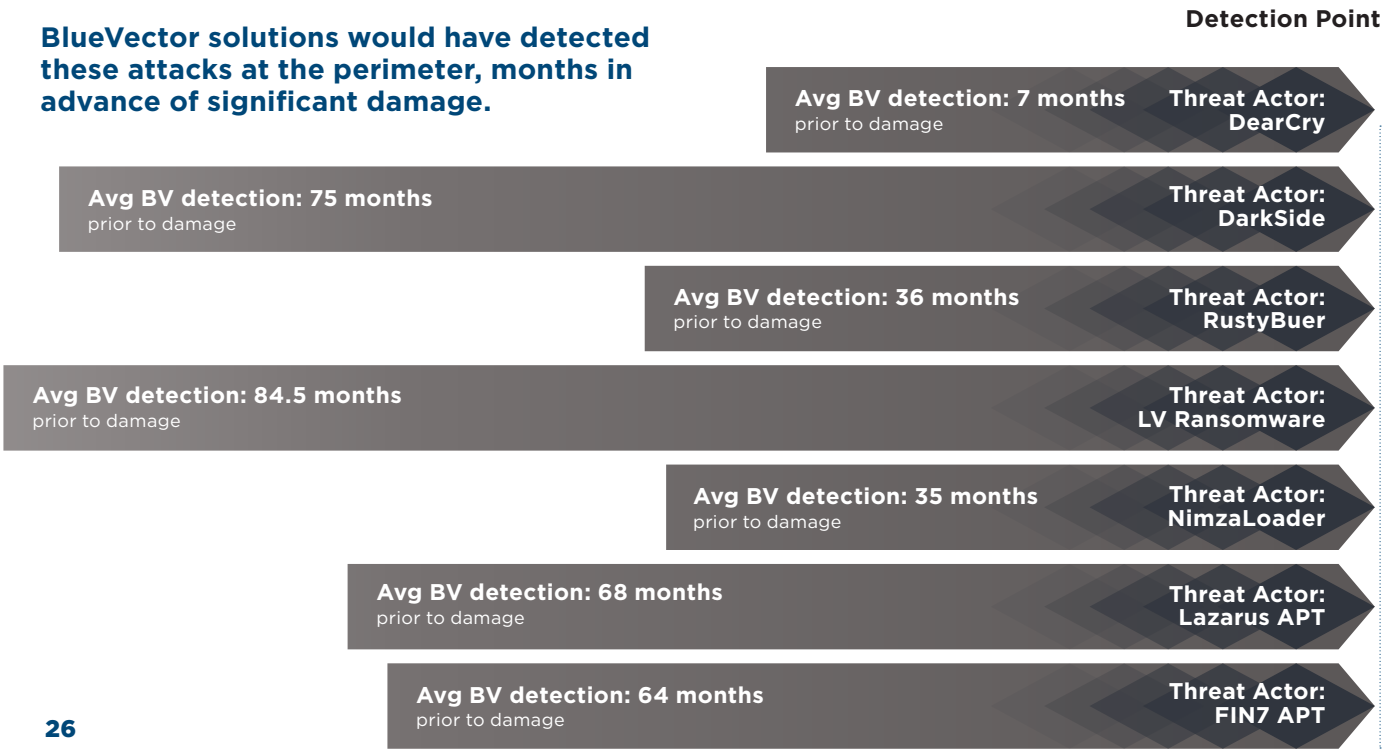
How Does FIN7 Propagate Lizar?

The malware does not contain the necessary code to self-propagate. Lizar claims to be an ethical hacking tool for Windows networks, in an effort to have it deployed on target networks.

When/How Did BluVector Detect It?

Sixteen samples related to Lizar are publicly available and BluVector's patented Machine Learning Engine (MLE) detected them all. Regression testing has shown the samples would have been detected an average 64 months prior to their release.

BlueVector solutions would have detected these attacks at the perimeter, months in advance of significant damage.



About BluVector ATD™

BluVector ATD is an advanced threat detection system that is transforming how security teams detect, triage and respond to security events.

As a machine learning innovator with more than a decade of experience applying AI to detect cyber threats, BluVector ATD strengthens the cyber defenses for some of the world's most discerning customers. With multiple patents, BluVector continues to help customers leverage AI-based approaches to manage the volume, velocity and polymorphic nature of today's and tomorrow's cybersecurity threats.

Included within BluVector ATD are two threat detection engines that work in parallel:

BluVector MLE

BluVector MLE is a patented supervised Machine Learning Engine that was developed within the defense and intelligence community to accurately detect zero-day and polymorphic malware in real time. Unlike unsupervised machine learning, which is leveraged by most security vendors today, BluVector MLE algorithms were pretrained to immediately identify malicious content embedded within common file formats like Office documents, archives, executables, .pdf, and system updates. The result: 99.1%+ detection accuracy upon installation.

BluVector SCE

BluVector SCE is the security market's first analytic specifically designed to detect fileless malware as it traverses the network. By emulating how the malware will behave when it is executed, the Speculative Code Execution engine determines, at line speed, what an input can do if executed and to what extent these behaviors might initiate a security breach. By covering all potential execution chains and focusing on malicious capacity rather than malicious behavior, the analytic technology vastly reduces the number of execution environments and the quantity of analytic results that must be investigated.