BLUVECTOR®
A COMCAST COMPANY

Relentless Ransomware: Threat Report Summary Second Half 2021

Contents

Based on our continuous observation and review of the threat landscape, ransomware attacks represented the most significant threats we tracked throughout 2021.

This is consistent with the almost daily reports on mainstream media of the latest ransomware attacks and the response of global law enforcement agencies and governments. Most cyber security professionals can relate to regularly receiving questions or comments regarding ransomware from family, friends and neighbors. This anecdotal evidence is backed up by **studies** showing global ransomware attacks in the first half of 2021 increased 151% compared to the same timeframe in 2020, and that the average cost globally for recovery from a ransomware incident has increased more than 100% in 2021 to $1.8 million[1].

After several high-profile ransomware attacks in the first half of 2021, the U.S. Treasury Department **announced a new counter-ransomware strategy in collaboration with its allies**, aimed at disrupting ransomware groups and their ability operate without consequence. These initiatives may be starting to have an impact in certain areas with ransomware groups. In fact, in the second half of 2021, ransomware attacks against healthcare providers are actually trending down. There is even evidence of schools being targeted less often. However, it's not all good news, attacks targeting manufacturing organizations are rising[2]. **Additionally, ransomware attacks are starting to increase in jurisdictions**

1. Acronis Cyberthreats Report 2022
2. *ibid*

which have been less aggressive about tackling the ransomware issue than the U.S., such as France and Germany. Estimates also place the total costs of ransomware to businesses exceeding $20 billion in 2021.

Most ransomware attackers see it as a profitable, relatively low risk business opportunity. However, with Western nations designating ransomware as a national security threat and devoting more law enforcement and intelligence assets to identify and prosecute the perpetrators, that risk may be more than some ransomware operators are willing to accept. We've seen at least some reports of ransomware groups going dormant as a result of increased enforcement. Already we have seen the REvil group "disappear" for a period of two months between July and September of 2021. This pattern has been observed before. Groups attracting too much law enforcement attention suddenly vanish, only to return a relatively short time later, often with a new name. We can expect this trend to continue.

Ransomware is, of course, far from the only malware threat despite it garnering the bulk of the attention. Although obvious, the prerequisite to being able to execute malware on victim systems is being able to deliver the malware to those systems.

We are seeing a rise in so called Access-as-a-Service providers.

Access-as-a-Service providers sell other attackers stolen, valid credentials to systems or access to already installed backdoors. Either way, it allows attackers an easy way to infect systems. Referring to it as a "service" is somewhat of misnomer as it's often a single transaction. In contrast, the now extremely common ransomware-as-a-service is a true service, where attackers pay the operators an ongoing subscription fee and/or a percentage of ransoms paid for access to the ransomware and its control panel. One of the Access-as-a-Service leaders has been the Emotet trojan who is mainly responsible for

the infection chain of the Trickbot trojan followed by Ryuk/Conti ransomware. As we described in a Threat Report detailed later in this summary, Emotet returned in November after disappearing in January 2021 as result of global law enforcement action.

And when it comes to access, one infection vector reigns supreme: Phishing Emails.

It's been reported almost 95% of malware is distributed via email. It's also the leading ransomware infection vector. Phishing emails use social engineering techniques to convince end users into clicking on links or opening attached documents. Further social engineering is used to convince the users into allowing the macros to execute. This is a tried-and-true technique that continues to be successful for attackers. In fact, this infection vector has been utilized by Emotet since it was first discovered in June 2014. This is despite increased security awareness training for users and advances in detection technologies. To attempt to evade detection, authors continue to evolve techniques. In a Threat Report, we looked at an IcedID trojan campaign which used an apparently benign macro. It did so by placing the malicious code in the body of the document, hidden behind an image, and placed other components in the document properties.

Though extremely popular, phishing is far from the only infection vector. In December we were reminded of the threat of a software vulnerability, especially when the affected software is widely used on internet facing systems. These vulnerabilities are easy and reliable to exploit remotely to execute an attacker's code. Our December 2021 **Threat Report** on the Apache Log4j library vulnerability noted attackers were quick to take advantage, initially to distribute coin miners and Mirai and Mustik bots.

2022 Outlook

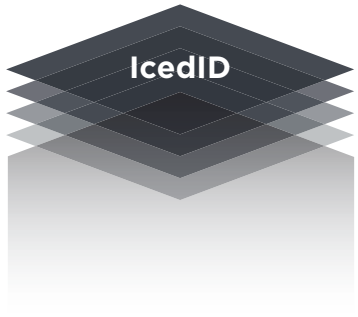
Any review of the threat profile of the second half of the year inevitably leads us to cast our gaze forward, to consider what the new year holds. Starting with the most obvious topic, ransomware, there's a chance that due to the focus from global law enforcement and governments it may have reached its absolute zenith. However, ransomware isn't going away any time soon. What we may see are less widespread and more focused ransomware campaigns. The first reason for this is some ransomware operators may choose to concentrate less on ransomware-as-a-service offerings, which are effectively open to the cybercriminal public and may therefore attract unwanted attention from authorities. Secondly, by utilizing more focused campaigns, there will be potentially less collateral damage, i.e., organizations the ransomware operators did not intend to target. Less collateral damage may again result in less attention from authorities.

As was the case in 2021, 2022 will clearly have more malware threats than just ransomware. However, attacker motivations will not significantly alter; the objective is profit. Cyber criminals pursue profit by many means, whether in direct monetary gains, such as ransom payments or theft of cryptocurrency wallets, or via theft of sensitive data and intellectual property. Both attacker and defender tactics will continue to evolve, perpetuating the ongoing cyber security race between them. As with every year, in 2022 it will be important to focus on the fundamentals of good cyber security practice. Humans will continue to be a weak link as attackers use of social engineering becomes more nuanced. Defense in depth is still as valid a practice as it has always been. Reliable, effective real time threat detection and hunting are essential. Finally, be wary of valid concepts which deviate from their original intent and become diluted once they are turned into buzzwords. For instance, while zero trust remains an extremely important journey for security organizations, unfocused or diluted versions of zero trust may cause more harm than good.

Threat Actors

2021 IcedID Update Uses Benign Word Macro to Evade Detection

Cyber criminals continue to modify the IcedID trojan attack chain to avoid detection and increase the pool of potential victims. IcedID operators have innovated their tactics to successfully defeat endpoint detection solutions. When tested, BluVector's Machine Learning Engine (MLE) would have detected an IcedID trojan sample 47 months prior to its release.



What Is It?

The IcedID trojan was the subject of a **Threat Report** soon after it first surfaced in 2017. Originally, Iced ID's primary purpose was to steal financial information, classifying it as a banking trojan. As it has evolved over time, this focus has widened to include distributing other malware as a dropper. IcedID continues to become more prolific, particularly since the success of international law enforcement's efforts to disrupt the notorious Emotet botnet's operations in January 2021. Throughout its life, IcedID's authors have regularly innovated and evolved the evasion tactics they employ, to ensure the maximum number of potential victims are successfully infected.

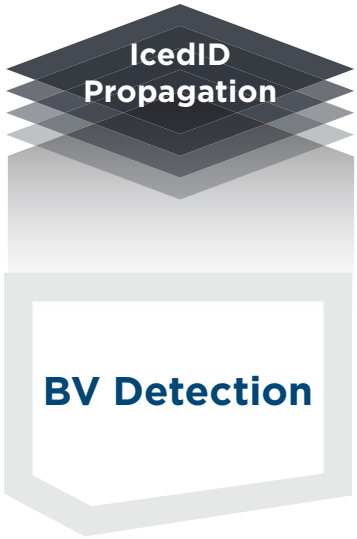
Previous examples of this include a campaign perpetrated in May 2020, which used a somewhat predictable COVID-19 pandemic related lure, married with an attack chain that used steganographic techniques to hide malicious executable payloads inside what initially appear to be harmless Portable Network

Graphics (PNG) format image files. Another campaign from April 2021 utilized malicious spreadsheet files containing Excel 4.0 macros, as described in **another recent Threat Report** relating to a Baz Loader campaign.

In this case, described in a recent report from researchers at Sentinel One, IcedID operators employed a technique that uses a Word document containing a macro which itself contained no malicious code to evade detection, particularly by endpoint-based security tools. Many macros used in malicious documents contain suspicious commands in the code of the macro itself, or incorporate various obfuscation techniques, which again make the macro appear malicious or at the very least suspicious. Here the macro itself is very basic and uses content from the document itself, as would a legitimate macro. Sentinel One's report doesn't include the actual Word document; however, the BluVector Threat Team identified and reviewed a sample using the identical technique and IOC's related to this campaign.

The malicious content is hidden behind an image file on the document itself which requests the user enable content so that the macro can execute. This content is actually an HTML Application file (HTA). The macro also uses the Title value from the document's properties to extract the destination filename for the HTA file. Once written out, the HTA file is executed. The HTA file contains JavaScript, and VBScript, to deobfuscate and execute JavaScripts to download the malicious IcedID DLL, save it with a JPG file extension, and execute it. The obfuscated JavaScripts are stored within the HTA file as base64 strings which are also reversed.

The IcedID DLL is used to collect and exfiltrate sensitive data from victim's system to the IcedID command and control (C2) site. The various tactics described above are aimed at evading endpoint detection solutions, to maximize the number of potential victims. It demonstrates IcedID's operators continue to evolve their tactics as part of their ongoing arms race with cyber defenders and detection solutions.



How Does It Propagate?

The malware does not contain the necessary code to self-propagate. The usual attack vector for IcedID campaigns is the use of phishing emails with malicious document attachments, and this was also the case for the campaign described in this report.

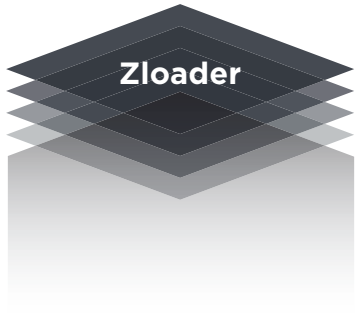
When/How Did BluVector Detect It?

Sentinel One's report included a list of nearly 500 hashes for the IcedID payloads associated with this campaign. Of these, 50 were regression tested with BluVector's patented Machine Learning Engine (MLE), which detected all of them. These samples would have been detected for an average of 78.5 months prior to their release.

Additionally, although their report didn't include any samples of the actual malicious Word documents, the BluVector Threat Team identified a sample using an identical mechanism described in the report and very likely part of the same campaign. When tested, BluVector MLE would have detected this malicious Word sample for 47 months prior to its release.

Variations on a Theme: Another "benign" word processing macro hides Zloader

Cyber criminals continue to rapidly adapt and change to evade detection. Criminals are evading signature-based detection tools, including end-point anti-virus. McAfee reports a campaign by nefarious actors designed to distribute the Zloader trojan using another example of a benign word processing macro. The attack begins with a phishing email containing a word processing doc and attachment.



What Is Zloader?

A previous Threat Report discussed a campaign to distribute the IcedID trojan using an attack chain that began with a word processing document containing a macro, which itself contained

no malicious code to evade detection. A recent report from researchers at McAfee details a campaign to distribute the Zloader trojan using a conceptually similar "benign" macro. Though the samples related to this campaign are four months older than those from the IcedID campaign.

The attack chain is a multi-step process:

- The target receives a phishing email containing a document as an attachment.
- If the user opens the document, they are presented with the expected message, advising them to enable content to view the document. This is the pre-requisite for allowing the macro to execute.
- If the macro is permitted to run, it uses content from Visual Basic forms in the document to access a remote password protected spreadsheet (XLS) document. This XLS document is stored memory and not written to disk.
- The macro uses content from the cells in the XLS document, to create a macro in the XLS document.
- The macro then alters the Windows Registry so that no warnings will be issued for executing Office macros.
- The macro then calls the macro created in the XLS document.
- The XLS macro downloads the Zloader DLL file and executes it.

The aim of this process is to evade detection by signature-based detection tools, including endpoint anti-virus. It attempts to achieve this by breaking up the content of macros, particularly any commands which would be classed as suspicious or malicious. This content, including the URL to download the XLS document from, is stored in different locations, such as in values for combo boxes on VBA user forms. By doing this, the macro, which is stored in the Word document appears, at first glance, to contain no problematic content. Not writing the XLS document to disk is another evasion tactic.

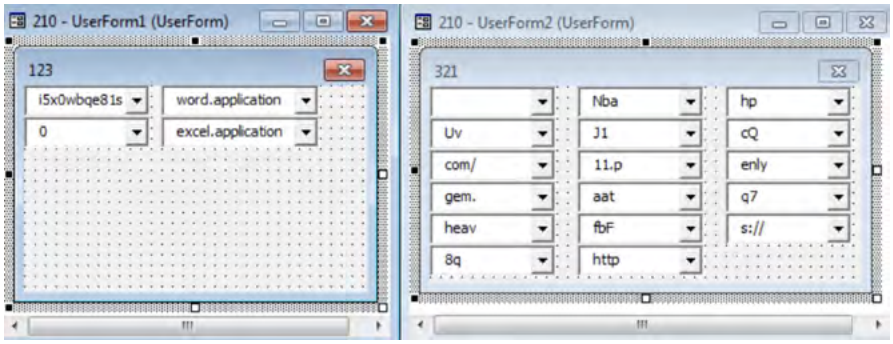
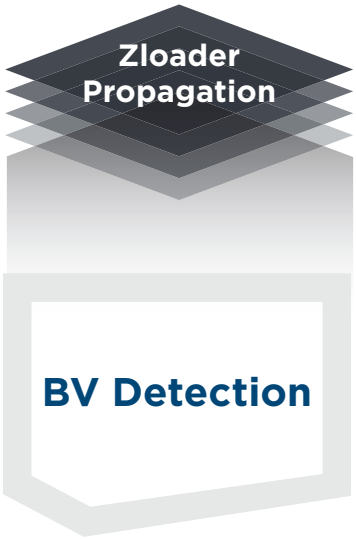


Figure 1: Zloader evasion using VBA UserForms

The McAfee report describes this as a new technique, though the samples related to this campaign were first seen in late January 2021. Additionally, during research for this Threat Report, a report released by the Threat Research team at Hornetsecurity was found. This report, released in late March 2021, describes a very similar attack chain to that described here, which resulted in the downloading and execution of a Zloader DLL; however, the initial attachment was a MHTML document. This MHTML document was given a "doc" file extension, ensuring it would be opened by Word, with the remainder of the attack chain and techniques matching those described above.

The fact these techniques are being described by research reports now, after being deployed since late January, suggests criminals are being successful at their intended purpose of signature-based detection systems. As a result, it can be expected, further variations on this theme will continue to be utilized by attackers, until they are forced to pivot to another technique to maintain the efficacy of attacks on their targets.



How Does It Propagate?

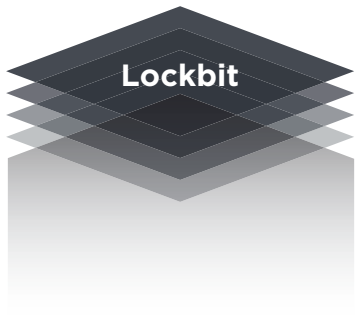
The malware does not contain the necessary code to self-propagate. This attack leverages social engineering, as the user must be convinced to allow the macro in the attached document to run, in order for this attack to be successful.

When/How Did BluVector Detect It?

Two samples are publicly available and BluVector's patented Machine Learning Engine (MLE) detected both. Regression testing has shown the samples would have been detected for an average of 52 months prior to their release.

Lockbit 2.0 Ransomware as a Service targets Operating System Domain Controllers

Cyber criminals unleashed a new propagation method that creates new group policies, increasing the threat networks. These group policies disable operating system antivirus protections and create a scheduled task on the endpoints to execute the ransomware. In addition to utilizing the double extortion threat of releasing stolen data unless a ransom is paid, Lockbit's operators also maintain a darkweb site with a list of their victims, a countdown to when the data will be leaked, and access to the data once the time has expired. Lockbit 2.0's ransom note also contains a message attempting to recruit unscrupulous employees or contractors to provide access to corporate networks for the Lockbit operators. These increased threats make it even more critical to ensure highly sensitive endpoints are properly secured.



What Is It?

A new variant of LockBit 2.0 ransomware unearthed by the **MalwareHunterTeam** contains a previously unseen propagation method. If the ransomware is executing on a domain controller, it can create new group policies which are deployed to all endpoints in that domain, disabling various protections and executing the Lockbit 2.0 ransomware. This capability represents an increased threat to one of the most commonly used networks and highlights the need to ensure highly sensitive endpoints, such as domain controllers, are properly secured.

First seen in September 2019, LockBit ransomware uses the popular ransomware-as-a-service (RaaS) model for distribution, via "affiliates" who are responsible for compromising networks and endpoints and then deploying the ransomware. A revenue sharing approach is used to split ransom payments between the affiliate and the LockBit operators, with 10-30% of the payments

going to the operators, dependent on the size of the ransom. It has been reported that in Q1 2021, LockBit held a 7.5% share of the ransomware market, third behind REvil and Conti. LockBit also follows suit with most other major ransomware operators by utilizing the so-called double extortion approach of threatening to release data stolen from victim's networks if they do not pay the ransom in a timely fashion. The LockBit operators maintain a darkweb site to list recent victims and how much time remains before their data will be released, it also allows for the downloading of data stolen from victims if the countdown has expired.

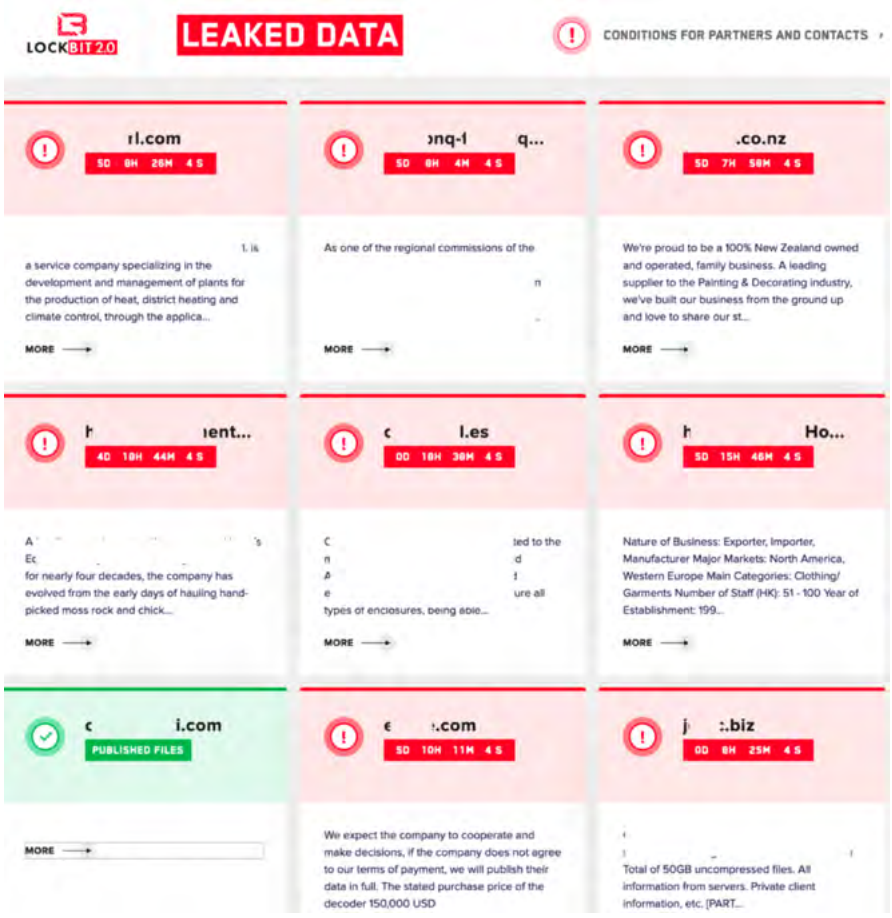


Figure 2: Lockbit Darkweb Site (Redacted)

A LockBit ransomware attack chain consists of an affiliate obtaining, or purchasing, access to a target organization's network. Once an initial foothold is established, the attacker will move laterally through the network, performing reconnaissance

to determine the highest value endpoints, such as file servers, and exfiltrating sensitive data to be used for double extortion purposes. Ordinarily, the attacker will also work to deploy the ransomware to as many endpoints as possible and synchronize execution of the ransomware to ensure the maximum number of files are encrypted. However, in this case, if the attacker can locate and compromise an operating system domain controller, LockBit 2.0 can use it to distribute new group policies to all endpoints in the domain. These group policies disable the operating system antivirus protections and created a scheduled task on the endpoints to execute the ransomware. Encrypted files are given the .lockbitfile extension, which is given its own icon, using the LockBit logo.

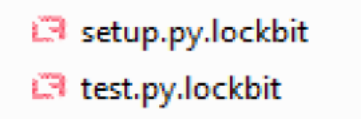


Figure 3: Encrypted files with .lockbit file extension

One interesting component of the Lockbit 2.0 ransom note, which is displayed by changing the wallpaper of the desktop of the infected endpoint, is that it contains a message (highlighted in the red rectangle in the figure below) attempting to recruit employees to provide access to corporate networks for the Lockbit 2.0 operators. The message begins by asking the question “Would you like to earn millions of dollars?”. While this might seem odd, given it is displayed on an infected system which is obviously part of an already compromised network, it is potentially aimed at unscrupulous external contractors who may have been called in to assist with the ransomware incident.

From a technical perspective, the LockBit 2.0 sample uses various techniques to attempt to evade detection and to make analysis more difficult. The method used by the sample to detect if it is being debugged is described in detail further below. As with other ransomware variants, the sample contains a large, encrypted list of process name strings which are terminated if they are found to be executing. These processes either relate to various

endpoint security and malware analysis tools or applications such as databases, mail servers and clients, and Office productivity suites. The latter group may have locked access to sensitive data files while they are executing, files which would be highly advantageous for an attacker to encrypt, including databases and mail and document files.

Another common malware tactic is to obfuscate the calls made to a API (Application Programming Interface), by not utilizing an import table and using one of several techniques to locate and call Windows API routines directly. LockBit 2.0 uses this tactic and others which mean that the structure of the executable itself is unusual. Windows executables use the Portable Executable (PE) file format, which is made up of specifically formatted headers and components called sections. Most .EXE files will contain sections which include **.text**, **.data**, **.rsrc** and **.reloc**, whereas LockBit 2.0 only contains **.text** and **.data**. The authors may have had many reasons for this, and while the sample is still a valid Windows executable, this approach does make the sample appear suspicious, particularly to a detection technology such as BluVector's patented Machine Learning Engine (MLE). The following figures show the sections found in the sample and those found in the executable for the Notepad utility.

When analyzing a malware sample, malware analysts and reverse engineers use a debugger to follow and control the execution of a sample. Obviously, malware authors are aware of this and employ various techniques to detect if a sample is being executed in a debugger. In the case of this sample, debugger detection is accomplished by checking the value of the NtGlobalFlag, which is a well-known, but infrequently used method. The NtGlobalFlag is a specific byte which is part of the Process Environment Block (PEB), a data structure which deliberately poorly documented by the developer, as it intended for use only by the operating system itself. The NtGlobalFlag byte is located at offset 0x68 in the PEB. If the sample is being debugged, the NtGlobalFlag will be set to 0x70, which can also be represented as a lower-case letter p.

The code from the sample checks the value of the NtGlobalFlag byte and if it shows the process is being debugged, the code will place itself in an infinite loop, which it achieves by having a JMP command jump to itself (highlighted in red in the figure below). This NtGlobalFlag check is the first code executed by the sample and is therefore obvious and is quite straightforward to circumvent.

How Does It Propagate?

The malware can propagate itself if it infects a domain controller, it can create new group policies and deploy them, resulting in the infection of all endpoints in that domain. The most common initial attack vectors for LockBit ransomware are compromised RDP (Remote Desktop Protocol) servers and phishing emails.

When/How Did BluVector Detect It?

Two samples are publicly available and BluVector's patented Machine Learning Engine (MLE) detected both. Regression testing has shown both samples would have been detected 91 months prior to their release in July 2021.

eCHoraix Ransomware targets QNAP and Synology NAS devices

Small Office/Home Office (SOHO) users and tech savvy consumers using QNAP and Synology Network Attached Storage (NAS) devices, are being targeted by cybercriminals with a newly released variant of the eCHoraix ransomware. The current attacks against QNAP devices make use of the CVE-2021-28799 vulnerability, first disclosed by QNAP on April 22nd,2021, which has previously been used to deploy variants of other QNAP ransomware. Researchers believe the initial variant of eCHoraix to target both QNAP and Synology devices was first developed in September 2020, prior to this, separate campaigns were used for each device type.

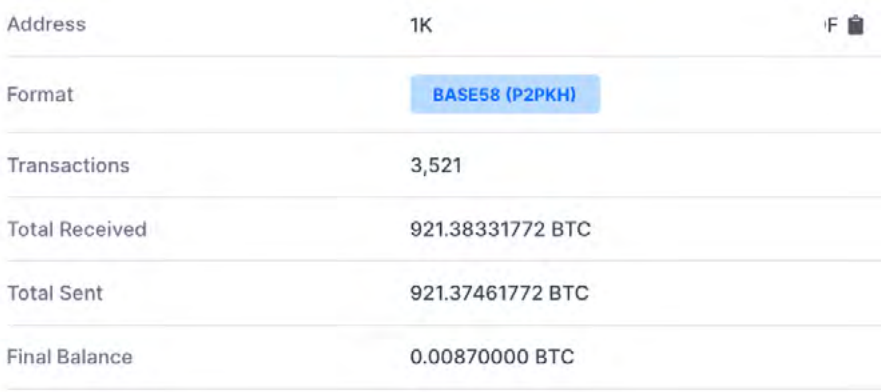
What Is It?

A newly released variant of the eCHoraix ransomware (previously also known as QNAPCrypt) has been found to target both QNAP and Synology NAS (Network Attached Storage) devices. Though not commonly used by large organizations, these devices are used by tech savvy consumers and SOHO users. QNAP and Synology are some of the most popular vendors in this market segment. Though SOHO users don't possess the financial resources to pay large ransoms, due to the potential lack of in-depth IT skills and support they may see paying a smaller ransom as their only option to regain access to their files. Researchers from Palo Alto Networks' Unit42 team have found the potential attack surface of internet facing QNAP and Synology NAS devices numbers nearly 250,000.

Originally released in June 2019, eCHoraix is written in the Go programming language and has been utilized in multiple campaigns, including significant campaigns in June of both 2019 and 2020. eCHoraix attacks have exploited vulnerabilities in QNAP operating system software as the attack vector on QNAP devices. In the case of Synology NAS devices, administrative account credentials with weak or default passwords are subjected to brute force and dictionary attacks to gain access. The current attacks against QNAP devices make use of the CVE-2021-28799 vulnerability, first disclosed by QNAP on April 22nd, 2021, which has previously been used to deploy variants of other QNAP ransomware. Researchers believe the initial variant of eCHoraix to target both QNAP and Synology devices was first developed in September 2020, prior to this, separate campaigns were used for each device type.

It has been reported by users of BleepingComputer's forums that each victim is given a different bitcoin address for the ransom payment. However, a forum user also noted that by following the transactions in the blockchain, it can be seen the ransom payments are always transferred to the same address. It's unknown if all the transfers to that address relate solely to

eCHoraix, however that address has received a total of more than 921 bitcoins, which at the time of writing was valued at approximately $US42 million.



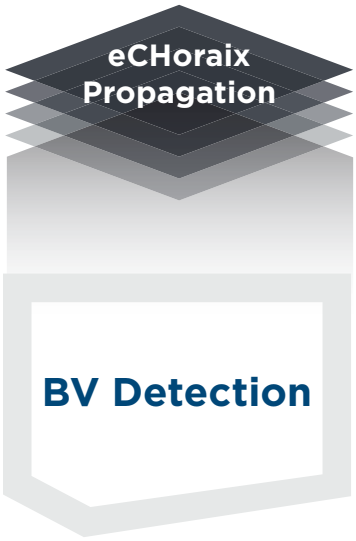
Address	1K F
Format	BASE58 (P2PKH)
Transactions	3,521
Total Received	921.38331772 BTC
Total Sent	921.37461772 BTC
Final Balance	0.00870000 BTC

Figure 4: Bitcoin address (Redacted)

Samples of this eCHoraix variant are compiled for either Intel or ARM architectures, as both processor types are used by different models in the QNAP and Synology NAS device ranges. When executed, the ransomware checks to ensure another copy isn't currently executing and hasn't previously executed on the device. It then contacts it's C2 (command and control) site to obtain the encryption key, ransom note text and the bitcoin address where the ransom is to be paid. Encrypted files are given the .encrypt file extension. The ransomware contains a large list of file extensions that it searches for and encrypts. The encryption process is handled in two stages, the first stage encrypts files matching a subset of approximately 40 file extensions which the authors clearly believe will be a priority to their intended victims. These priority file extensions relate to source code, image, and document files. The remainder of file extensions are then searched for and encrypted.

eCHoraix ransomware is an example that cyber criminals are not solely focused on large organizations as targets. They are aware that SOHO users and businesses represent a profitable target, albeit at a smaller per capita profit. They're also cognizant of the fact that these targets can be considered soft, with strong motivation to pay the ransom, due to a lack of IT resources and

support and a heavy reliance on the data that may be encrypted. It also illustrates that cyber security basics, such as prompt patching and good password hygiene, are critical to organizations of all sizes and every user.



How Does It Propagate?

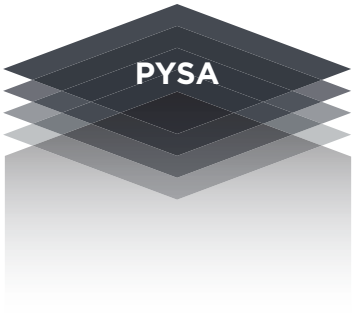
The malware does not contain the necessary code to self-propagate. In the case of QNAP devices, exploitation of the CVE-2021-28799 vulnerability is the attack vector, and for Synology devices it is brute-forcing of administrative account credentials.

When/How Did BluVector Detect It?

Ten publicly available samples, compiled for both Intel and ARM architectures, were regression tested against BluVector patented Machine Learning Engine (MLE). All samples were detected, for an average of 8.3 months prior to their release into the wild and up to 17 months.

PYSA Ransomware is not your Amigo

With amigos (friends) like this on the dark web, who needs enemigos (enemies)? PYSA ransomware, an acronym for *Protect Your System Amigo*, was one of the top four most common ransomware variants in Q2 2021. PYSA are another ransomware player of some significance, who have leaked sensitive data from almost 200 organizations. PYSA is being offered by its operators to "partners" using the Ransomware as a Service (RaaS) model. The RaaS model is popular with cyber criminals as it provides a division of labor between the ransomware authors and their partners. The operators create and update the ransomware itself, as well as any backend necessary, and the partners compromise victims' networks, exfiltrate sensitive data and deploy the ransomware. They then split any ransom payments, with the majority going to the partners.



What Is PYSA?

PYSA has been listed in recent reports as one of the top four most common ransomware variants in Q2 2021 and has not previously been the subject of a Threat Report. PYSA ransomware is an evolution of Espinoza ransomware, which was first seen in October 2019, with the first PYSA variant surfacing in December 2019. It is offered via the common RaaS model, with the operators providing the ransomware for a cut of the profits, leaving the "partners" to compromise victim organization's networks, exfiltrate sensitive data, deploy the ransomware and execute it.

As with most other ransomware operators, PYSA operators host a dark web site where they post sensitive data stolen from victims on the "Partners" page, the data is listed under the heading of "Something interesting from our partners". For this Threat Report, a review of the site was performed. **Please Note**: No stolen data was accessed or downloaded during this review. The site, which uses the font and color scheme of an MS-DOS application, lists 189 victim organizations whose data was released, covering the period April 2020 to August 2021. For each victim, various zip files are provided for download, with the file listing for each zip file also able to be displayed. Based on the names of the files present in these zip files, there appears to be a wide variety of sensitive personal, financial, and business information. This data suggests that data exfiltration is one of the primary objectives of the PYSA operators and partners.

A review of the victim organizations listed on the dark web site shows most of them are located in the United States, with the United Kingdom, Brazil, Italy, and Canada the most common of the remaining 24 countries. A breakdown of victim organizations based on industry found Education the most common, followed by *Medical, Manufacturing, Construction and Local Government*. There is no evidence to determine if these target profiles apply equally to all PYSA victims, or only those who did not pay the ransom in time. The following tables list the country and industry breakdowns in full.

Victims	Country
107	United States
15	United Kingdom
11	Brazil
9	Italy
8	Canada
6	France
4	Spain., Australia
3	South Africa, Columbia, Germany
2	Argentina, Switzerland
1	Ireland, Romaina, Israel, Kenya, Netherlands, Norway, Slovakia, Saudi Arabia, Denmark, Belgium, Indonesia, Mexico

Figure 5: List of victim organizations by country

Victims	Industry
33	Education
24	Medical
23	Manufacturing
23	Construction
14	Local Government
13	Transportation
12	Financial
10	ICT
9	Food Services
7	Legal Services
7	Retail
3	Mining, News Media
2	Religion, Facilities Management
1	Military, Real Estate, Sports, Hospitality

Figure 6: List of victim organizations by industry

As for the ransomware itself, it does not contain any significant anti-analysis or evasion mechanisms, in fact the list of file extensions which are to be encrypted are hardcoded in plain text into the ransomware. This could be because PYSA tactics seem to place an emphasis on exfiltrating sensitive data from victim's networks prior to deploying the ransomware. As such, the attackers will likely have visibility to which anti-virus solution is in use and can ensure that the ransomware will not be detected by that product. Therefore, the PYSA authors don't see the need to invest large amounts of time and effort into sophisticated code. PYSA uses the Crypto++ library for cryptographic functions, rather than the common practice of using the cryptographic libraries which are part of Windows. Encrypted files are given the **.pays** file extension. Files which are 1KB or less in size are not encrypted, regardless of their file extension.

Rather than change the endpoint's desktop background to an image of the ransom note, PYSA uses a novel technique. It changes the value of the *LegalNoticeText* and *LegalNoticeCaption* entries in the operating system registry so that the ransom notice is displayed at each reboot. These values are normally used to present users a notice of conditions of use for a system when logging on. The ransom note is also placed in a text document named Readme.README, dropped in every directory on the system.

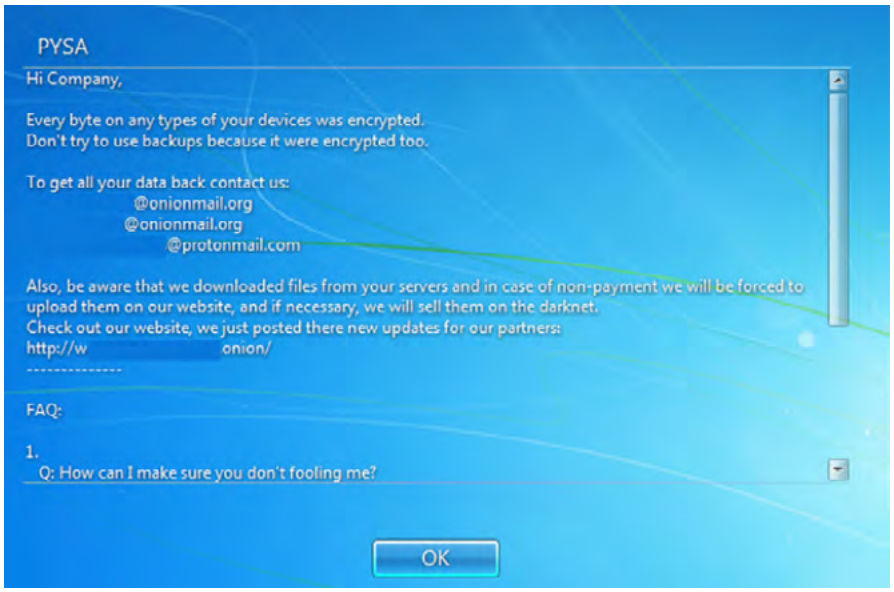


Figure 7: Ransom note displayed as the legal notice (Redacted)

PYSA are another ransomware player of some significance, who have leaked sensitive data from almost 200 organizations. Whether these organizations couldn't afford to pay the ransom or recovered their data via other means, it appears the data contained in these files would constitute a data breach for each of these organizations. This is an example that the threat of releasing sensitive information is often potentially a greater motivating factor for victim organizations to pay ransoms than regaining access to encrypted files, as they may have alternative means to achieve that, such as backups.

How Does It Propagate?

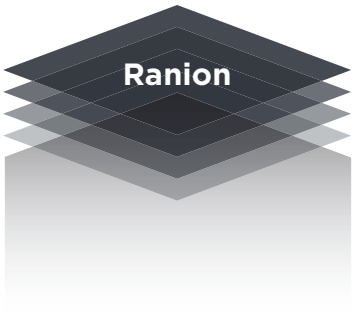
The malware does not contain the necessary code to self-propagate. The most common attack vector for PYSA ransomware is brute force attacks against poorly secured, internet facing, RDP (Remote Desktop Protocol) and AD (Active Directory) servers.

When/How Did BluVector Detect It?

Fifteen recent, publicly available PYSA samples were regression tested with **BluVector's patented Machine Learning Engine (MLE)** and it detected them all, with an average detection time of 31.33 months prior to their release.

Ranion: The Slow and Steady Approach to RaaS

Ranion ransomware practices strategic patience to the detriment of its victims. Ranion ransomware relies on the RaaS (Ransomware as a Service) model, but with a twist. It doesn't expect its customers to share any ransomware profits resulting from the use of its malware. Criminals can subscribe to the service at different levels. Researchers found a bitcoin wallet associated with Ranion has received approximately $4.7 million in deposits, not bad for a product the disclaimer states is "for educational purposes only".



What Is It?

For obvious reasons ransomware attacks frequently gain headlines in the mainstream press. As a result, specific ransomware families and their authors can receive more coverage and scrutiny than they might like. Often, due to a particularly high profile or sensitive victim, a ransomware attack draws the focus of law enforcement or intelligence agencies. When this happens, the ransomware attacker often chooses to go dark, either temporarily or permanently. After returning from a temporary shutdown, attackers often attempt to rebrand to avoid further unwanted attention from government entities and security researchers. High profile ransomware follows the "make hay while the sun shines" approach, aiming for maximum profits over a relatively short period. Researchers from Fortinet have recently described their analysis of Ranion, a ransomware family which takes an opposing slow and steady approach.

Ranion ransomware was first discovered by a researcher from Radware Security in early Feburary 2017. Since its inception, Ranion has utilized the RaaS (Ransomware as a Service) business model, albeit with a different approach to the larger, well known ransomware operators. The most obvious difference is that Ranion operators only charge a subscription fee to use the ransomware, they do not take a share of any ransoms that victims pay. Most RaaS operators withhold at least 20% of ransoms

collected as a commission, they use a sliding scale which may go as high as 40%. Currently, Ranion offers four subscription levels: "Elite," and "Premium," are both for 12-month periods and cost $1,900 and $900, respectively. There is also a "Standard" subscription, lasting 6-months and costing $490. Lastly a "Test" subscription is $120 for a month.

One interesting add-on to subscription packages, though it is included in the "Elite" package, is the "Dropper" option. This allows attackers to specify a remote file, which Ranion will download and execute after the file encryption process is complete. In most cases, attackers will choose to install some sort of backdoor, such as a RAT (Remote Access Trojan). If a victim pays the ransom and decrypts their files, this additional malware is not removed, giving the attacker continued access to the infected systems. They could choose to make use of this access directly or sell it on to other attackers.

Ranion ransomware is most frequently distributed as a zip file attached to a phishing email. This is hardly the most sophisticated infection vector, suggesting Ranion is likely used by lower skilled attackers. However, it is a vector that continues to be successful, regardless of the level of awareness training provided to the victim's employees. Based on a code analysis, it appears Ranion is based on HiddenTear, a freely available open-source ransomware proof of concept. Ranion samples also make use of the ConfuserEx .NET protector, which makes reverse engineering more difficult and also obfuscates the functions and purpose of the code, enhancing its chance of not being detected by legacy anti-virus solutions. Recent Ranion samples encrypt 44 different file extensions, with the .wallet extension recently added to target crypto currency users and provide them with significant motivation to pay the ransom. Ranion's operators will also add additional file extensions to be encrypted at no charge upon request.

Ranion ransomware is not sophisticated, nor has it claimed any high-profile victims. However, it has seemingly carved out a niche

for itself, mostly under the radar, allowing it to continue operating for more than 4 ½ years in an endeavor which is not normally know for longevity. Researchers found a bitcoin wallet associated with Ranion has received approximately $4.7 million in deposits, not bad for a product the disclaimer states is "for educational purposes only".

How Does Ranion Ransomware Propagate?

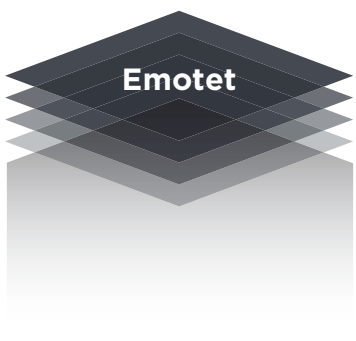
The malware does not contain the necessary code to self-propagate. Consistent with Ranion's target market of lower skilled attackers, the attack vector for the majority of Ranion attacks is phishing emails with zip file attachments containing the ransomware.

When/How Did BluVector Detect It?

Twenty-five publicly available Ranion samples were regression tested against **BluVector's patented Machine Learning Engine (MLE)**. All samples were detected, and would have been detected an average of 87 months prior to their release.

Emotet Returns With a Strong Sense of Déjà Vu

The Emotet trojan is back! The banking trojan first discovered in 2014 has evolved and is enabling other malware groups to effectively attack victims. As in the past, recent Emotet attacks have employed word processing and spreadsheet documents. How often do you receive those? A total of 12 publicly available samples related to recent Emotet attacks were regression tested against BluVector's patented Machine Learning Engine (MLE), and all were detected.



What Is It?

Multiple reports in recent weeks have detailed the reemergence of the Emotet trojan, after a multi-national law enforcement operation in January 2021 effectively shut down Emotet operations.

First discovered as a banking trojan by researchers from Trend in June 2014, Emotet has continuously evolved since that time. Emotet operators have found the greatest success by utilizing Emotet to provide access and downloader services to other malware groups. The most well-known of these collaborations is the attack chain that begins with Emotet, which facilitates installation of Trickbot malware, which in turn results in the installation and execution of Ryuk ransomware (the predecessor to Conti ransomware). Emotet became so successful that in the announcement of its shutdown in January 2021, Europol described it as the "world's most dangerous malware". In their shutdown announcement, the U.S. Department of Justice noted there were more than 1.6 million infected systems globally, with over 45,000 of those located in the U.S.

For such a prolific and notorious threat, Emotet has utilized a fairly basic attack chain, which has remained largely unchanged over time. The current Emotet reemergence continues this trend. The Emotet attack chain begins with a spam email which has a word processing or spreadsheet document attached. This document contains a malicious macro, which if the user can be socially engineered into allowing to run, will result in the downloading and execution of the Emotet malware. The operators have continued to rely on this attack chain for one simple reason, it continues to work for them - not only in terms of overall numbers of victims, but the specific target profile of victims sought by the other malware groups that utilize their services.

The recent Emotet attacks have utilized both word processing and spreadsheet documents. When opened by the user, as expected, they both present messages to the user instructing them to enable editing and/or enable content, as this is necessary to allow the embedded malicious macros to execute. As can be seen in the following screenshots, the Excel document message even contains a typo, referring to EXCELL with two L's.

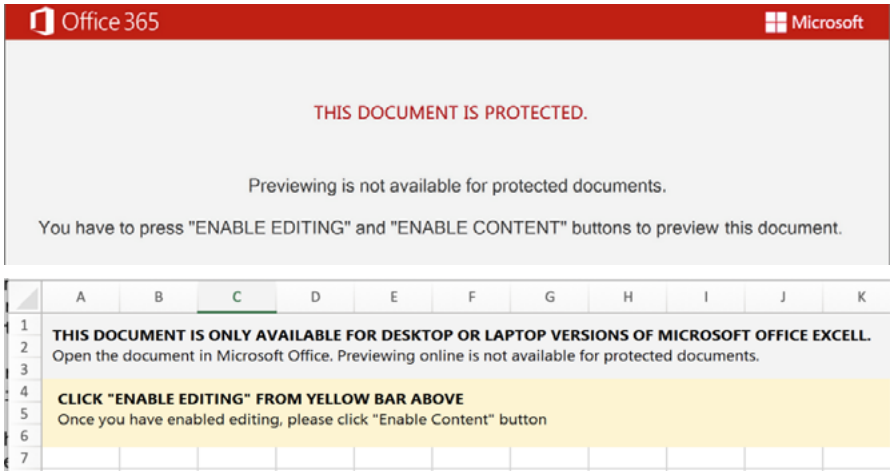
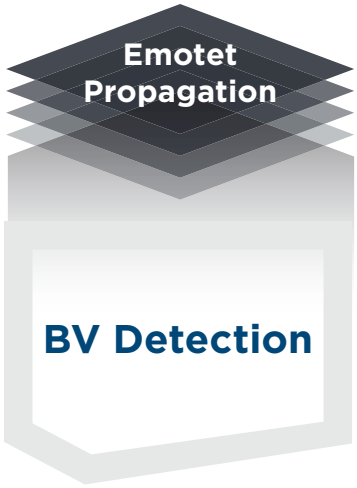


Figure 8: Messages presented to users when opening the documents.

In the samples analyzed for this Threat Report, the macros in the documents were identical. The macro itself is fairly straightforward and uses minimal obfuscation. It contains a Powershell command string, which is obfuscated by being liberally interspersed with the string “Cew”.

The purpose of the Powershell script it is to attempt to download and execute the Emotet malware itself, from one of seven URL’s hardcoded into the script.

The reemergence of Emotet is not surprising, in fact it could have been considered almost inevitable. It has been reported the Ryuk/Conti ransomware group was the driving force behind this return, as clearly their bottom line was taking a hit due the lack of a reliable provider of initial access and downloader services. However, it is concerning that Emotet has returned with the same attack chain, which is neither novel nor sophisticated. This is of concern as clearly in many organizations, their employees are still being taken in by basic social engineering and their detection infrastructure is still relatively easily evaded. Emotet operators are taking an if-it-ain’t-broke-don’t-fix-approach, as it would appear from their point view, so far it ain’t broke.



How Does It Propagate?

The malware does not contain the necessary code to self-propagate. Emotet attacks begin with spam emails which have documents attached containing malicious macros.

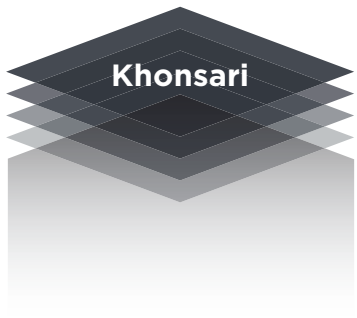
When/How Did BluVector Detect It?

A total of 12 publicly available samples related to recent Emotet attacks were regression tested against BluVector's patented Machine Learning Engine (MLE), and all were detected. The three DOCX samples would have been detected 53 months prior to their release, the two XLSX samples would have been detected 45 months prior and the eight Emotet malware DLL samples would have been detected for 71 months prior.

Khonsari – A new strain of malware delivered via the Apache Log4j RCE Vulnerability

Since the recent, successful exploitation of the Log4j RCE vulnerability, the number, and variety of malware payloads exploiting this vulnerability has continued to increase. An unseen strain of malware, known as Khonsari, is one example of the new payloads.

Regression testing of the Khonsari sample shows that BluVector would have detected it 44 months prior to its release.



What Is It?

As we described in our **previous Threat Report**, attackers are utilizing successful exploition of the **Apache Log4j RCE vulnerability** as an infection vector to install their malware payloads. As expected, following publication of that Threat Report, the number and variety of these malware payloads has continued to increase. One such payload, described by several researchers, was a previously unseen strain of malware, Khonsari, so named for the file extension added to files it encrypts.

Analysis of the Khonsari sample, performed as part of the research for this Threat Report, was more interesting than anticipated. Firstly, unlike most of the malware payloads installed by exploiting the Log4j vulnerability, this sample executes on , rather than on Linux. Also noteworthy, the sample is a small (13KB), .NET executable and does not implement any significant anti-analysis techniques. Meaning that from an analysis point of view, the sample decompiles cleanly. This indicates the sample was created by a relatively unsophisticated threat actor, which is consistent with the relative ease with which the Log4j vulnerability can be exploited.

The most significant attempt at anti-analysis by the authors, is merely to utilize a basic string obfuscation technique. In more technical terms, strings within the sample are obfuscated by XOR'ing each string with a unique key, consisting of an eight character, alphabetic string. A simple Python script was written during analysis in order to reverse the obfuscation. The decrypted strings are shown below, along with their specific key:

```
VyDBLfRt :  AQAB
ZsfHtxUW :  lPy6RT6hgfRmVkajw3ZwFCAb2nZBCHJka3xkmeknG7SA/
aAct9urvSY5fCEfC7HDMkw+x4UNyueXa3rPM7GTHZuQSegmdOyNk-
G29hi+LhKCH4...
ZrvabgFb :    ---
FtxHwtyx :  Fec*****iques.Properties.Resources
IXrKEAOE :  \HOW TO GET YOUR FILES BACK.TXT
ObukVnAe :  Your files have been encrypted and stolen by
the Khonsari family.
            If you wish to decrypt , call (225) 287-****
or email k****khonsari@gmail.com.
            If you do not know how to buy btc, use a
search engine to find exchanges.
            DO NOT MODIFY OR DELETE THIS FILE OR ANY EN-
CRYPTED FILES. IF YOU DO, YOUR FILES MAY BE UNRECOVERABLE.
            Your ID is:
QvhhaQoW :  .khonsari
ItAGEocK :  .ini
diYplLvh :  ink
GoaahQrC :  http://3.145.115.94/zambos_caldo_de_p.txt
qMIamfMA :  C:\
mRQjIJGG :  Downloads
zBlcAGJA :  .khonsari
```

Figure 9: Khonsari Decrypted Obfuscation

Once the strings are deobfuscated and the code that utilizes them is reviewed, they reveal some interesting behaviors. First, the string “ink” appears to be a typo. The code snippet below shows that filenames ending with the deobfuscated strings “.khonsari” and “.ini” are skipped, however it is unlikely the author’s intention was to skip files ending with “ink.”It is more probable that this string was intended to be “lnk”, the file extension for shortcut files.

Next, a command is executed which is intended to download the contents of a URL to a string. However, in this case, the result is not assigned to a string. More significantly though, there is no error handling for this command. Therefore, in practice, if this URL is unreachable – as it was during analysis – the malware will crash. It’s unclear whether the authors intended this to function as a kill switch for the malware or not. Regardless, blocking access to this URL removes any threat this malware poses, as the encryption process has not yet begun at this point in the code.

However, it is the strings which are partially redacted in the list above that are the most interesting of all. The name of the resource included in the sample, the contact phone number, and email address in the ransom note are those of a legitimate business located in Baton Rouge, Louisiana. The contact phone number for the legitimate business has been changed since this malware was released, indicating they received a degree of unwanted attention as a result. It i common practice for malware authors to include blocks of text within their code. These are easily altered between variants and are used in an attempt to evade signatures created to detect previous versions of the malware.

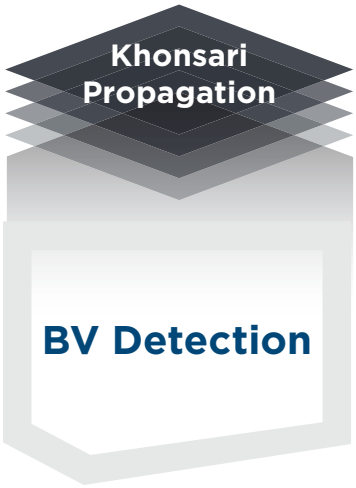
In this case, it seems to achieve a completely different objective. It doesn’t provide the victim a way to contact the threat actor in order to negotiate, or pay, the ransom. The sample utilizes cryptographically secure encryption, meaning encrypted files cannot be decrypted with a valid decryption key. Therefore, the sample’s behavior actually characterizes it as destructive malware,

not ransomware. It is not clear whether this malware is intended to be purely destructive, or if it is actually ransomware under active development, and this was a test of sorts.

```
FtxHwtyx : Fec*****iques.Properties.Resources
ObukVnAe : Your files have been encrypted and stolen by the
Khonsari family.
If you wish to decrypt , call (225) 287-**** or email
k****khonsari@gmail.com.
If you do not know how to buy btc, use a search engine to
find exchanges.
DO NOT MODIFY OR DELETE THIS FILE OR ANY ENCRYPTED FILES.
IF YOU DO, YOUR FILES MAY BE UNRECOVERABLE.
Your ID is:
```

Figure 10: Khonsari ransom note

Reverse engineering malware is often a lengthy process, requiring highly skilled and experienced individuals. This sample shows that the required reverse engineering effort can be proportional to the sophistication of the malware being analyzed. It also demonstrates that a sample may behave differently to how it appears on first glance. Finally, it is a reminder that sophisticated threat actors and malware are not necessary to cause damage to an organization's infrastructure.



How Does It Propagate?

The Log4j RCE vulnerability, **CVE-2021-44228**, is used as the infection vector in these attacks. This malware does not contain the necessary code to self-propagate.

When/How Did BluVector Detect Khonsari?

The publicly available sample of Khonsari malware analyzed for this Threat Report was tested against BluVector's patented Machine Learning Engine (MLE), and it was detected. Regression testing of this sample shows that BluVector would have detected it 44 months prior to its release.

About BluVector

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.

BLUVECTOR®
A COMCAST COMPANY

As a leader in advanced threat detection, BluVector is empowering security teams to get answers about real threats, allowing businesses and governments to operate with greater confidence that data and systems are protected.

Learn More or Schedule a Demo at bluvector.io