UNITRENDS
unitrends.com

A BEGINNER'S GUIDE TO RANSOMWARE

What IT Pros Need to Know

WARNING: With this eBook, Unitrends lends insight about how simple and prevalent ransomware attacks have become. It lets readers know how sophisticated and successful cybercriminals have become. DO NOT try this at home

Contents

Overview

FACT: Ransomware Hackers Collected over $1 BIllion in 2016

Imagine being part of an IT segment with sky-rocketing growth, increasing success with massive deployment worldwide and revenues expected to triple in 2017 from the $1 billion it brought in for 2016. It's an industry that is constantly evolving with new versions of the software being released and deployed every day.

We're talking about ransomware, a form of malware that locks up customer's data. The malware programming community continues to infiltrate and block access to more and more devices expanding the web of victims. Then ransomware distributors demand payment in exchange for a key to unlock the encrypted files, bringing in billions of revenue.

- Locks victims' files with strong unbreakable encryption
- Demands payment for a private key to unlock data

Barrier to entry for the industry is very low. Open Source versions of the software are available to anyone who wants to tap this lucrative market. The emergence of these open source ransomware programs hosted on GitHub and hacking forums is expected to further spur the growth of these attacks in 2017.

"Even if the wannabe perpetrator doesn't have the skills to create their own malware from free code, this can now also be readily outsourced. There is already a ransomware as a service [RaaS] model that provides automatically generated ransomware executables for anyone who wants to get rich by infecting potential victims. The bottom line is that creating or buying your own ransomware has never been easier. So ransomware is here to stay and is expected to be a bigger problem yet in 2017," said Warwick Ashford,[5]

RaaS is a variant of ransomware that is user-friendly and it can be easily and quickly deployed. You can download the software either for free or a very low fee. The goal is to trick targets into infecting their computer or generate even more revenue by locking an organization's network. Customers then get sent a ransom and payment deadline, and if the victim pays up,

> "These programs are freely available for anyone who has the basic knowledge needed to compile existing code."
>
> **Ondrej Vlcek,**
> **Chief technology Officer**
> **Avast.**

60% of enterprises have been hit by ransomware[1]

63% were down more than a day[2]

70% paid the ransom[3]

40% of spam contains ransomware[4]

the original author gets between 5% to 30% "commission"—and the rest goes to person who launched the attack.

The FBI *officially* recommends that companies not to give in to ransomware demands, but off the record they'll say, pay the money if you need the data. Meanwhile, an IBM security study release in December concluded that 70% of businesses hit with ransomware paid a ransom to regain access to files.

1. CNBC
2. CB Insights
4. North American Enterprise Survey and Calculator
4. Tech50Plus.com
5. ComputerWeekly.com Jan 2017

ADVANCES IN RANSOMWARE

A Glimpse into the Latest Updates by Cybercriminals

New Attacks

Advances in Ransomware

UPDATES & PROMOTIONS

Teaser Key Codes,
Localized Versioning and More...

There are always energizing advances from ransomware merchants. Here's a glimpse at what's new. *Get 1 Free – Code* proves to targets that their files can be unlocked by sending them one free decryption. Malware distributors now offer voice enabled versioning, plus, new options for hacking Mac computers. New functionality means enterprises now deal with threats of potential data leaks. This is big stuff for hospitals who have regulatory requirements to protect information and it is very significant to any company that has a database of credit card or social security information. They just have to pay to avoid legal and financial nightmares.

Some of the more successful promotional strategies include the creation of geo-targeted messaging.

Local-focused emails that are designed to entice downloads. Imagine getting a download request from your neighborhood bank! You'd open it right?

Philadelphia Ransomware has their own promotional video on You Tube, offering free lifetime updates with purchase. They brand themselves as the "most advanced and customizable ransomware ever.

There are new "no executable" versions of ransomware that use a combination of scripting languages to encrypt the files on a customer's machine. The encryption, the ransom note, and call out to a command and control server are completed without an executable file. These ransomware families are able to avoid detection of many traditional security vendors because they are taking advantage of legitimate processes on the system. Everything they do registers as "legitimate."[7]

New Variations

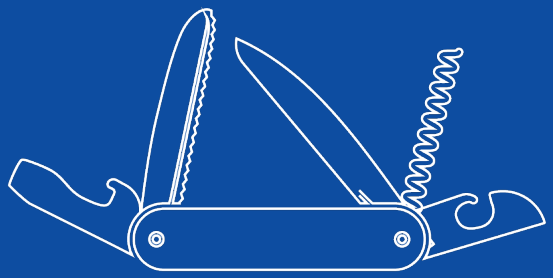
Havoc performs routines typical of a ransomware type that uses symmetric and asymmetric cryptography to encrypt its targeted files. [6]

Satan is offered as RaaS which is promoted as a free ransomware kit that requires a simple registration. Satan targets 131 types of files and appends them with a .stn extension. The program is set up so that the distributor gets 70% of the ransom paid and the developer gets 30%. [6]

VxLock targets files and appends the extension name .vxlock to its encrypted file. It has AntiVM, Anti-debug and Anti-Sandbox features. [6]

LataRebo Locker prevents its victims from using their computers by using a large image containing the ransom note. It adds entries to the Windows Registry to enable activation whenever the user's operating system starts up. It will also add additional registry entries that disables the task manager, preventing users from terminating its process. [6]

6. Ransomware Recap, TrendMircor, March 2017.
7. Recordedfuture.com Jan 2017



TOOLS OF THE RANSOMWARE TRADE

Insight into How Easy It Is to Be a Cybercriminal

Gidgets & Gadgets to get started

Ransomware Resources

BITCOIN ALLOWS HACKERS TO REMAIN ANONYMOUS

Over 30 Merchant Services Accept Bitcoin

FACT: The US Government estimates that there are 4,000 ransomware attacks released daily

Resources for do-it-yourself ransomware attacks are plentiful. Part of the financial success of ransomware can be credited to the ability of the hacker to be anonymous online. Payment is made as a non-traceable electronic payment. Bitcoin has become a widely accepted currency. There are over 30 merchant services that manage bitcoin transactions including:

1. Bitaps.com
2. BitBayPay
3. Bitcoin Transaction Coordinator
4. BitcoinPay
5. Bitcoinpaygate
6. BitKassa .
7. BitPagos
8. BitPay
9. BitPOS
10. BitStraat SiteCite:
11. Luno API
12. Blockchain.info
13. Blockonomics
14. Coinbase
15. CoinBox
16. Cashila
17. CoinCorner
18. CoinGate
19. Coinify
20. CoinPip
21. Coinsnap
22. Cryptopay
23. Cubits
24. Gourl.io .
25. Lavapay
26. OKPAY
27. PayFast
28. Paxful
29. Rocketr
30. SpectroCoin .
31. SpicePay
32. XBTerminal

Some of the major software contributors in the ransomware arena include:

- Cryptolocker
- TorrentLocker
- CryptoWall
- CBT-Locker
- TeslaCrypt
- Locky
- Unbreakable Encryption
- AES
- RSA
- Curve" ECC
- Network to C&C Server
- Tor
- 2P
- POST/HTTPS
- Hardcoded URLs

"

Your personal files are encrypted!

Your important files produced on this computer: photos, videos, documents, etc. have been encrypted. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for the computer. To decrypt files you need to obtained the private key.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

CryptLocker

"

NOTE: One of the more successful "Welcome" messages is posted above.

BIG MONEY HACKS

Some Victim Stories

Companies that paid up

Big Money Hacks

THE BIGGER THEY ARE...

Ransomware Turns to Big Targets—
With Even Bigger Fallout

FACT: Even the FBI recommends paying the ransom if backups are not in place. That's how hard it is to defeat ransomware if you haven't protected your data ahead of time.

70 percent of business victims paid the hackers to get their data back, a recent study found. Of those who paid, 50 percent paid more than $10,000 and 20 percent paid more than $40,000.[8]

Some Examples of Big Hacks:

- Ransomware attack led Los Angeles Valley College (LAVC) to fork over $28,000 after they realized that a ransomware infection left them with no way to recover their organization's encrypted data.

The college released a statement verifying the success of the attack, "In consultation with district and college leadership, outside cybersecurity experts and law enforcement, a payment was made by the District. It was the assessment of our outside cybersecurity experts that making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost." [9]

- In late May, at the University of Calgary, a ransomware attack crippled multiple systems connected to the university's network. The school decided that it was the best course of action to pay the $20,000 demanded by the attackers because of the risk to critical data and valuable research. [10]

> "To be honest, we often advise people just to pay the ransom [if they don't have backups].
>
> **Joseph Bonavolonta**
> **Asst. Special Agent**
> **FBI Cybercrime Boston Division**

- Hollywood Presbyterian Medical Center. In 2016 they paid the equivalent of $17,000 to resolve a ransomware infection. The ransomware didn't just encrypt files but severely affected operations for about 10 days, forcing staff to go back to paper records and fax machines. They had backups, but were unable to recover from them. [11]

- In the Austrian Alps, Romantik Seehotel Jägerwirt Brandstaetter, hotel was unable to issue new key cards to guests who arrived during the 24 hours that the hotel's reservation system was down. They were forced to pay the ransom of about $1,600 USD. [12]

8. CNBC, Ransomware spiked 6,000% in 2016 and most victims paid the hackers
9. The Washington Post Jan 2017
10. TheStar.com Canada, June 2016
11. LA Times, Feb. 2016
12. The Daily Mail Fan. 2017

BACKUP VENDORS ARE TRYING TO SCARE IT PROS

Vendor Efforts to Sell More Product

Trying to sell defense

Backup Vendors are Trying to Scare IT Pros

AFRAID OF A LITTLE HACKER?

The vendor strategy

Why are IT backup vendors trying to scare IT pros?

Backup vendors are trying to alarm IT pros to the point that they'll buy their software to fend off attacks. But the fact is, not all backups are safe. Windows-based backup vendors are more vulnerable to ransomware. Since ransomware programs are designed for Windows, files backed up on Windows are also a strategic target. Organizations are using the cloud to store data and ransomware programmers have created ransomware that can infect files kept in the cloud. Some ransomware strains, including a variant of Virlock, which actually uses the desktop sync clients of popular cloud services to access and encrypt files stored in the cloud. For example, if the Google Document a person is working on locally gets encrypted, the encrypted file will sync with Google Drive. Bottom line, cloud storage is not backup. Backup means another *protected* off-site copy of the data

While ransomware teams try to garner revenue from any platform target, the preponderance of Microsoft Windows systems makes them far and away the most lucrative prey.

On the flip side, the folks at Unitrends are starting to scare malware distributors. They've developed a ransomware detection process that really makes it tough to mount a successful attack. They now offer:

- Proactive discovery of recovery issues, caused by ransomware,
- Adaptive & predictive analytics against backup data designed to search for ransomware threat conditions
- Proactive alerting when ransomware conditions are detected

> "My prediction going forward is that we're not only going to see ransomware focused on data, we'll see more ransomware focused on other ways to disrupt a business. [12]
>
> **Marcin Kleczynski**
> **CEO, Malwarebytes**

To date there are enough IT Pros who are sitting on the sideline or using Windows backup that there's plenty of viable targets.

13. Wired.com Feb 2017

UNITRENDS 5 ARMS OF DEFENSE

A Look at How Unitrends Fends Off Ransomware

UNITRENDS
unitrends.com

Undefeated v. Ransomware

Unitrends Helps Defeat Ransomware 5 Ways

5 DEFENSE ARMS

Protect. Secure. Test.
Detect. Recover

PROTECT

Unitrends provides both local and cloud protection options, Giving customers 3-2-1 protection, 3 copies of your data - 2 different types of media - 1 copy off-site.

SECURE

The transition away from malware susceptible Windows backup software to a purpose-built hardened Linux solution exponentially hampers hackers from successful attacks. By running on a hardened Linux platform Unitrends Recovery Series backup appliances that are resistant to malware and ransomware attacks.

There are over 100 million known viruses for Windows. Linux is still diverse and difficult to penetrate because it is hierachical.[15]

TEST

A key component of Unitrends portfolio's security capability is Unitrends Recovery Assurance. It provides automated testing of recovery for backups — both local and in the cloud.

Recovery Assurance secures the recoverability of mission critical applications; recovery will occur in the time required to meet an organization's IT service demands, no matter what causes the disaster or outage, whether planned or unplanned.

DETECT

Uses adaptive & predictive analytics against backup data designed to search for ransomware threat conditions. Algorithms use machine learning to forecast ransomware conditions. Proactive alerts are sent when ransomware conditions are detected.

> "It's...easier than ever to deploy. To carry out such a diversity of attacks, hackers have created hundreds of strains of ransomware, Many are variations on readily available "off-the-shelf" malware. [14]"

RECOVER

Unitrends Instant Recovery lets their customers spin up their backup data on-premisses in minutes, thereby, deflecting any attempted attacks.

Unitrends has created an iron-clad security platform, a virtual force field, to ensure that the digital assets of their client's are protected. The mantra for hacking Unitrends customers, "Don't waste your time."

14. Wired.com, Ransomware Turns to Big Targets—With Even Bigger Fallout
15. Dunn, John E. ComputerWorldUK. Jan. 2016

UNITRENDS
unitrends.com

UNITRENDS CUSTOMERS DETECT AND DEFEAT ATTACKS

Unitrends Customer Success Stories

Proven Struggles

Unitrends Customers Detect and Defeat Attacks

NO RANOMWARE PAID

Unitrends customers have *always* recovered from ransomware attacks

There's a mounting pile of evidence that indicates that malware distributors can't impact Unitrends customers with ransomware.

Gerson Company is a wholesale importer for retailers. They were just rolling along and then they got attacked. It was a BitLoker hack. There were ransomware demands popping up and files being locked all over their network on pc and laptops. "When we went to investigate that is when we found the answer to what was going on with the network files. This all took place over a period of about half a day." reports Watkins. Fortunately, with Unitrends Recovery [Series]... Gerson is able to make frequent backups to ensure a short Recovery Point Objective (RPO). Going to recent backup they were able to recover...their files ." says Watkins.

Bethleem Schools in NY was a ransomware target twice. Malware merchants got the message to users that they had to pay ransom and that their files were encrypted. They called the attempt trivial and quickly restored their system from Unitrends backups.

Mandurah Catholic College was hit by hackers but they had Unitrends Backup software. They said that having Unitrends Backup allowed their small IT team to beat the attack with minimal disruption and stress.

Life's Abundance makes healthy pet food products. An attack was launched to see if there was an opportunity to collect a healthy-sized ransom. But it was right after they installed Unitrends, Malware got in when a user clicked a bad attachment which shut down two workstations and many accessible file server shares. But with the Unitrends Recovery Series, within two hours they were fully operational again.

Ransomware vendors took on **Broadway Carpets**, not for their pile rugs, but for a pile of cash. Hackers encrypted their files while the IT guy was out fishing. By the time he came back every folder on their server was encrypted. But a few weeks before the attack, they installed Unitrends Backup software. So from his cell phone the guy found a restore point and was back up and running in 30 minutes.

> "We've had *two* separate ransomware incidents where users informed me that their files were encrypted with a message about paying a ransom. It was trivial and quick for me to restore the data from the Unitrends backup"
>
> **Gary Halbedel**
> **Network Administrator**
> **Bethlehem Central School District**

Boston Architectural College had a ransomware infection on their network. Several hundred gigs of data were affected. But they backup their data every hour. And by using the Unitrends UI, they were back up and running in 20 minutes.

The Force Field of Ransomware

True technology leaders set the bar instead of fighting to keep up with the pack. While ransomware pros continue to develop new techniques, Unitrends is transforming the business by preventing successful ransomware attacks with an onslaught of game-changing defensive mechanisms for their users. They've created a virtual force field to stop attacks.

For ransomware distributors there are so many laggards who have failed to keep pace with the technology that plenty of prime targets are vulnerable and susceptible to ransomware attacks. A quick recap:

- **OPPORTUNITY:** Ransomware is a billion dollar industry and growing. 70% of attack victims pay the ransom. Ransomware vendors just need to find victims.
- **NEW & IMPROVED:** Advances in programming are ongoing. Functionality of attack software and new versioning continues to enhance revenues.
- **TOOLS OF THE TRADE:** RaaS options, bitcoin merchants and open source software mean lots of potential for new hackers joining the fray.
- **BIG MONEY HACKS:** The bigger they are the harder they fall. When big organizations with big important data get hacked, they need to pay the big ransom.
- **SCARED IT PROS:** Company's with security platforms try diligently to alert IT pros to the fact that they are prime ransomware targets. For the time being, either IT pros are ignoring the warnings or they're adding insufficient protection. So the ransomware business remains strong.
- **UNITRENDS:** Bottom line: Unitrends has this figured out from 5 different angles, literally. However, there are plenty of enterprises who have yet to install Unitrends and are highly susceptible to ransomware attacks.

UNITRENDS
unitrends.com

Your next step

To discover how Unitrends can help you defeat ransomware five ways

Explore Unitrends Products

Discover the industry leading products and services online at unitrends.com

Download a free 30-day trial

Sign-up now and claim your free 30-day, no risk trial of Unitrends Backup Software with ransomware detection

See the #1 All-in One Enterprise Business and Continuity Solution in action.

Register for a live demo.

UNITRENDS

unitrends.com

PART# WP-2059-ENG-A