Ransomware: don't expect a full recovery, however much you pay

27 APR 2021 4

Ransomware

Previous: Naked Security Live – J... Next: Gamers update! Nvidia patc...

by Paul Ducklin

When it comes to all the various types of malware out there, none has ever dominated the headlines quite as much as ransomware.

Sure, several individual malware outbreaks have turned into truly global stories over the years.

The *LoveBug* mass-mailing virus of 2000 springs to mind, which blasted itself into hundreds of millions of mailboxes within a few days; so does *CodeRed* in 2001, the truly fileless network worm that squeezed itself into a single network packet and spread worldwide literally within minutes.

There was *Conficker*, a globally widespread botnet attack from 2008 that was programmed to deliver an unknown warhead on April Fool's Day, but never did. (Conficker remains a sort-of unsolved mystery: no one ever figured out what it was really for.)

And, there was *Stuxnet*, discovered in 2010 but probably secretively active for years before that, carefully orchestrated to spread via hand-carried USB drives in the hope of making it across security airgaps and into undislosed industrial plantrooms (allegedly Iran's uranium enrichment facility at Natanz).

But none of these stories, as dramatic and as alarming as they were at the time, ever held the public's attention as durably or as dramatically as ransomware has done since the early 2010s.

Send money, or else

Ransomware, of course, probably ought to be called "extortionware", "blackmailware" or "menaceware", because that's precisely what it does: "*Send money, OR ELSE.*"

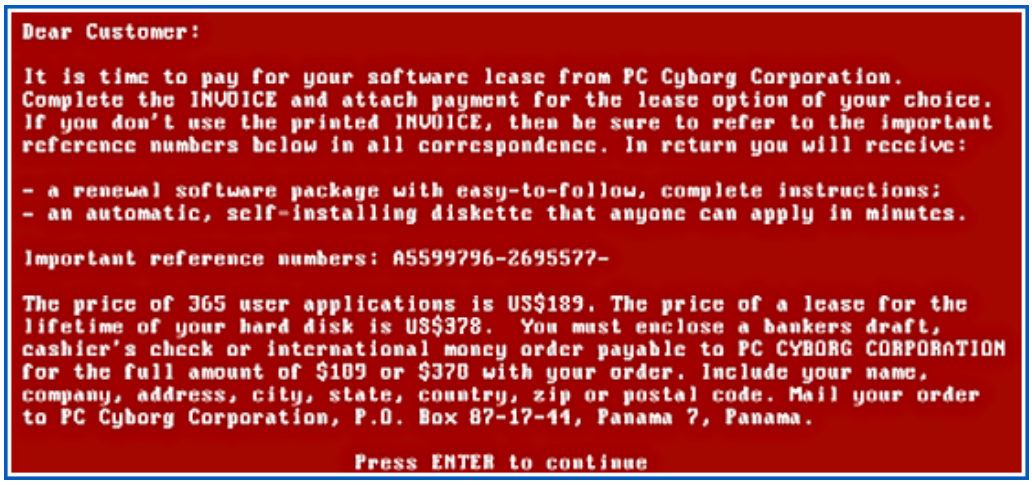
Interestingly, ransomware first raised its ugly head way back in 1989, when a software program that was supposed to be an AI system to give advice about HIV and AIDS was sent to tens of thousands of unsuspecting victims all over the world...

...only to scramble their files 90 days later and demand the payment of $378 by international money order to an accommodation address in Panama.

If you paid up, said the malware, you would be sent an unscrambling program that would decrypt your ruined files and restore your computer to its pre-infection state.

Or so the malware author claimed.

Fortunately, due to the difficulty and expense of distributing the malware in the first place (the AIDS information Trojan was snail-mailed on floppy diskettes), collecting the money via the international banking network, and sending out the "fix" program, ransomware remained a rarity for the next 25 years.



Blackmail page from the 1989 AIDS Information Trojan.

Follow the money

Unfortunately, once cryptocurrencies such as Bitcoin became well-known and comparatively easy to use, cybercriminals adopted them enthusiastically as an ideal tool for collecting extortion payments.

That was back in about 2013, when the infamous CryptoLocker malware appeared, and the cyberunderground has thrown itself vigorously into creating and spreading ransomware ever since.

Boy, how the ransomware scene has changed since then.

Blackmail demands in 2013 were typically about $300 per PC, with ransomware attacks aimed broadly at everyone and anyone, one computer at a time, whether the victim was at work or at home.

In 2013, CryptoLocker gave each individual victim 72 hours to pay $300.

Now, ransomware gangs typically go after entire networks, breaking into them one-by-one and preparing for a moment (typically timed for when the network IT team is asleep) when all the computers are scrambled simulataneously.

In attacks like this, where organisations may be brought to a complete operational halt, the extortion demand may be as high as millions of dollars in a single payment, in return for a "fix" for the entire network.

Even worse, many ransomware gangs take the time to upload (or to steal, to put it more bluntly) as much corporate data as they can before scrambling it, and they add this nasty detail into their blackmail notes.

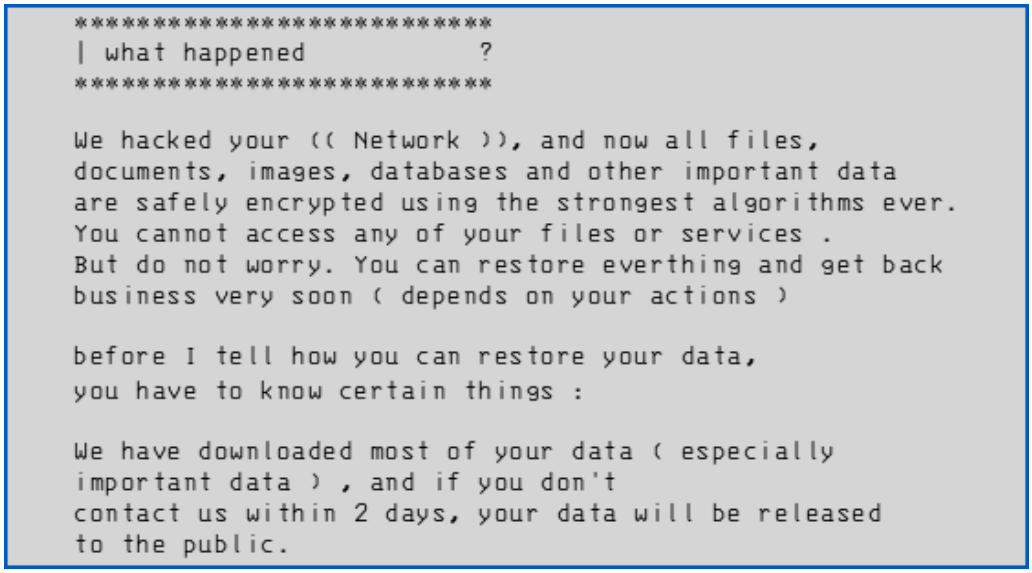
Instead of simply, "*Send us money, OR ELSE you won't see your files again,*" the criminals are saying, "*Send us money, OR ELSE we'll sell off all your trophy data to the highest bidder, or send it to your competitors, or upload it to the regulator, or taunt your*

customers with it, or dump it for everyone to see, or all of the above. Oh, and you won't see your files again, either."

In fact, many ransomware gangs run their very own "negative PR" portals on the dark web, where they publish the confidential data of victims who don't pay, or blog about how bad their victims' cybersecurity was, or both.

In other words, even if the encryption part of the attack fails, or if you have a backup from which you can recover your computers without paying up, the criminals can and will demand money with menaces anyway.

As we said above, ransomware really ought to be called "blackmailware", not least because the crooks have figured out how to make their crime pay even when there's no data that they're actually holding to ransom.



```
**************************
| what happened          ?
**************************

We hacked your (( Network )), and now all files,
documents, images, databases and other important data
are safely encrypted using the strongest algorithms ever.
You cannot access any of your files or services .
But do not worry. You can restore everthing and get back
business very soon ( depends on your actions )

before I tell how you can restore your data,
you have to know certain things :

We have downloaded most of your data ( especially
important data ) , and if you don't
contact us within 2 days, your data will be released
to the public.
```

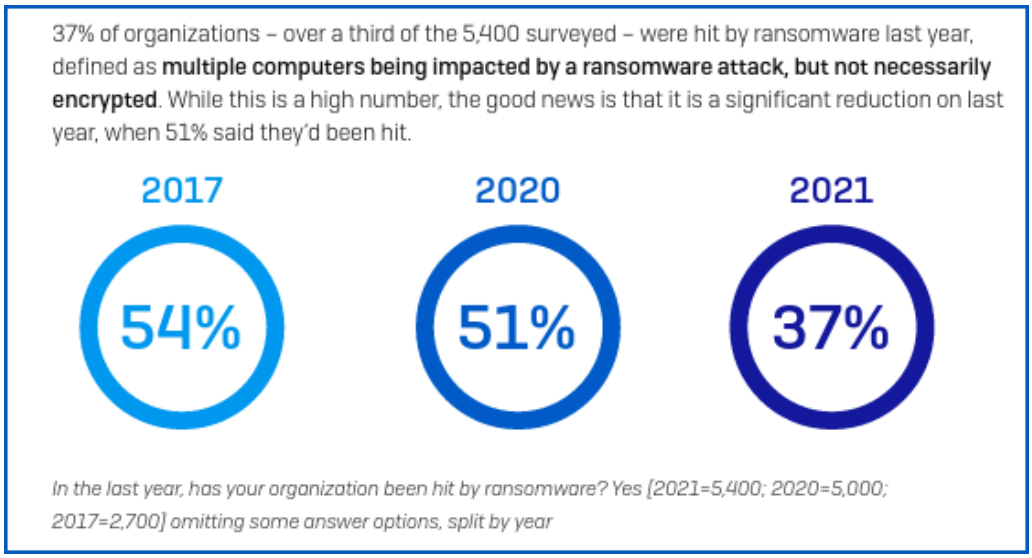
Blackmail note from 2021 BlackKings ransomware threatening a deliberate data leak.

Here's the good news

The good news is that, as part of our ongoing efforts to track the evolving ransomware scene, we've just published our very latest

State of Ransomware report for 2021.

And the percentage of respondents who said they did get hit was noticeably lower than in 2020, when we published our previous report, and lower still than in 2017, when we did our first.



Source: Sophos "State of Ransomware 2021" report.

The bad news, of course, is that "only 37% got hit" is the the good news, because "more than a third" is still a disappointingly large proportion of those surveyed.

There are many fascinating, and probably quite surprising, facts that are revealed out in the report, which is why we strongly recommend that you read it now.

For example, of companies that either decided to pay up (e.g. thinking it would be quicker), or were forced to do so (e.g. because their backups turned out to be useless)...

...about one-third of them got less than half their data back, and (in an intriguing flip of the numbers), about half of them lost more than a third of their data.

A truly unfortunate 4% of victims who paid up got nothing for their money at all, and only 8% claim to have recovered everything after

submitting to the blackmail.

In blunter words: 92% of victims lost at least some data, and more than 50% of them lost at least a third of their precious files, despite paying up and expecting the crooks to keep their promise that the data would be restored.

Broken promises

Remember also that an additional "promise" you are paying for in many contemporary ransomware attacks is that the criminals will permanently and irrevocably delete any and all of the files they stole from your network while the attack was underway.

You're not only paying for a positive, namely that the crooks will restore your files, but also for a negative, namely that the crooks won't leak them to anyone else.

And unlike the "how much did you get back" figure, which can be measured objectively simply by running the decryption program offline and seeing which files get recovered, you have absolutely no way of measuring how properly your already-stolen data has been deleted, if indeed the criminals have deleted it at all.

Indeed, many ransomware gangs handle the data stealing side of their attacks by running a series of upload scripts that copy your precious files to an online file-locker service, using an account that they created for the purpose.

Even if they insist that they deleted the account after receiving your money, how can you ever tell who else acquired the password to that file locker account while your files were up there?

> If the crooks buried the upload password on a command line or in a configuration file that they copied around your network during the attack,

any number of other threat actors could have stumbled upon it before, during or after the attack, even if the crooks didn't intend to share it with anyone else.

What to do?

- **Read the report.** The figures tell an interesting and important story about the scale and the nature of the danger posed by ransomware. By reading the report, you're getting an insight into what victims are experiencing in real life, not merely what the cybersecurity industry is saying about the threat.
- **Assume you will be attacked.** Ransomware remains highly prevalent, even though the relative numbers are down from 51% last year to 37% this year. No industry sector, country, or size of business is immune. It's better to be prepared but not hit, than the other way round.
- **Make backups.** Backups are the still the most useful way of recovering scrambled data after a ransomware attack that runs its full course. Even if you pay the ransom, you rarely get all your data back, so you'll need to rely on backups anyway. (And keep at least one backup offline, and ideally also offsite, where the crooks can't get at it.)
- **Use layered protection.** Given the considerable increase in extortion-based attacks, it's more important than ever to keep the bad stuff out and the good stuff in.

Follow @NakedSecurity on Twitter for the latest computer security news.

Follow @NakedSecurity on Instagram for exclusive pics, gifs, vids and LOLs!

Free tools

Sophos Home
Protect personal PCs and Macs

Hitman Pro
Find and remove malware

Previous: Naked Security Live – J... Next: Gamers update! Nvidia patc...

4 comments on “Ransomware: don’t expect ...

Jeff April 27, 2021 at 6:38 pm

I recall that in the early 80’s, prior to July 1985, there was talk about ransomware that specifically targeted the data of a popular accounting software package that ran on the Apple II. It was supposed to encrypt the data files, but allow the program to access them for several weeks before cutting off its own background decryption, making the backups pretty much useless, and then would make a ransom demand for the decryption key.

Anyone else hear of that?

2 0 Rate This

Reply

Jack Wilborn April 27, 2021 at 6:52 pm

Duck one, nice... uh, that’s Duck, nice one... As a retired reserve police officer I always figured the victims didn’t get much for the

money. I'm actually surprised it's this much. Nice article.

3 0 Rate This

Reply

Business Directory April 29, 2021 at 3:18 pm

The apparent decline in the number of organizations being hit by ransomware is good news, but it is tempered by the fact that this is likely to reflect, at least in part, changes in attacker behaviors.

0 0 Rate This

Reply

Paul Ducklin April 29, 2021 at 4:35 pm

And, of course, the nature of any decline from 51% to 37% of anything depends rather heavily on what that "anything" is.

If you lived in a high-tax country and the government reduced the personal income tax rate from 51% to 37%, that would be one thing. But if you had an unreliable car and the chance of it breaking down on any journey "improved" from 51% to 37%...

...you'd still be walking home an awful lot.

1 0 Rate This

Reply

What do you think?

Comment

Name

Email

Website

Post Comment

Recommended reads

APR
15 BY PAUL DUCK 0

S3 Ep28: Pwn2Own hacks, dark web hitmen and COVID-19

FEB
03 BY SALLY ADAI 2

What should you say if you have a data breach? Catch up with Jason

MAR
22 BY HARRIET ST 1

Instagram scams and how to avoid them