The rise of targeted ransomware

nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/

By Mark Stockley

11 Sep 2018

*Thanks to **Peter Mackenzie** of Sophos Support for his behind-the-scenes work on this article.*

In the year since the "shock and awe" of WannaCry and NotPetya – outbreaks that spread globally in a matter of hours – ransomware has been making a lot less noise.

You'd be forgiven for thinking that it's had its day, but reports of the demise of ransomware have been greatly exaggerated, as they say.

While cryptomining and cryptojacking have been sucking all the air out of the press room, a snowball that started rolling well before anyone had ever heard of WannaCry has been gathering pace and size.

The snowball is a trend for stealthier and more sophisticated ransomware attacks – attacks that are individually more lucrative, harder to stop and more devastating for their victims than attacks that rely on email or exploits to spread.

And they do it in a way that's hard to stop and easy to reproduce.

WannaCry's reliance on an exploit stolen from the NSA (the USA's National Security Agency) made its success hard to replicate, and its promiscuous spread attracted the attention of law enforcement everywhere while leaving countless copies of the malware to be analysed by researchers and security companies.

The criminals behind targeted ransomware attacks have no such limits. They rely on tactics that can be repeated successfully, commodity tools that are easily replaced, and ransomware that makes itself hard to analyse by staying in its lane and cleaning up after itself.

And while the footprint of a targeted attack is tiny in comparison to an outbreak or spam campaign, it can extract more money from one victim than all of the WannaCry ransoms put together.

Targeted attacks can lock small businesses out of critical systems or bring entire organisations to a grinding halt, just as a recent SamSam attack against the city of Atlanta showed.

For every Atlanta-style attack that hits the headlines though, many more go unreported. Attackers don't care if the victims are big organisations or small ones, all that matters is how vulnerable they are.

In fact, the three examples of ransomware we've chosen for this article, Dharma, SamSam and BitPaymer can be thought of (allowing for considerable overlap) as ransomware aimed at small, medium and large businesses respectively.

All businesses are targets, not just ones that hit the headlines.

For example, a recent investigation by Sophos revealed that SamSam's apparent preference for the healthcare and government sectors was an illusion. The majority of the SamSam victims uncovered in the investigation were actually in the private sector but none of them had gone public, whereas some government and healthcare victims had.

The anatomy of a targeted attack

The specifics of targeted attacks evolve over time, vary from hacking group to hacking group, and can be adapted to each individual target. Despite that, they show remarkable similarity in their overall structure.

In a typical targeted attack, a criminal hacker:

1. Gains entry via a weak RDP (Remote Desktop Protocol) password.
2. Escalates their privileges until they're an administrator.
3. Uses their powerful access rights to overcome security software.
4. Spreads and runs ransomware that encrypts a victim's files.
5. Leaves a note demanding payment in return for decrypting the files.
6. Waits for the victim to contact them via email or a dark web website.

The similarity between attacks and attackers isn't the result of coordination, but a convergence around a method that works reliably, netting the criminals using it huge payoffs.

That convergence goes as far as including details like special offers: while the ransoms they demand vary significantly, Dharma, SamSam and BitPaymer attacks all offer their victims the opportunity to decrypt one or two files for free to prove that they can do it – ransomware's equivalent of a kidnapper's "proof of life".

Although the outline of each attack is very similar, scripted even, what makes targeted attacks so fearsome is that the attackers are on hand to adapt and improvise.

In a targeted attack the assailant's job is to break into the victim's network and maximise the chances of the ransomware succeeding in its malevolent task, and the adversary most likely to ruin the attacker's day is security software operating as one of several layers of overlapping protection.

Writing ransomware that isn't detected by security software is no easy task, so attackers will often look for a way to outflank it by exploiting operating system vulnerabilities that let them elevate their privileges.

If they can make themselves an administrator, an attacker will be permitted to run powerful administration tools, like third party kernel drivers, that can disable processes and force delete files, bypassing the protections put in place to stop the attackers uninstalling security software directly.

Security software still isn't helpless though. Set up correctly, it can defend itself by blocking the legitimate third party utilities that might be used to undermine it.

Variations on a theme

The coup de grâce in a targeted attack comes when the attacker has manoeuvred themselves into a strong enough position to run their ransomware unencumbered.

Now lets look at some of the ransomware itself.

Dharma

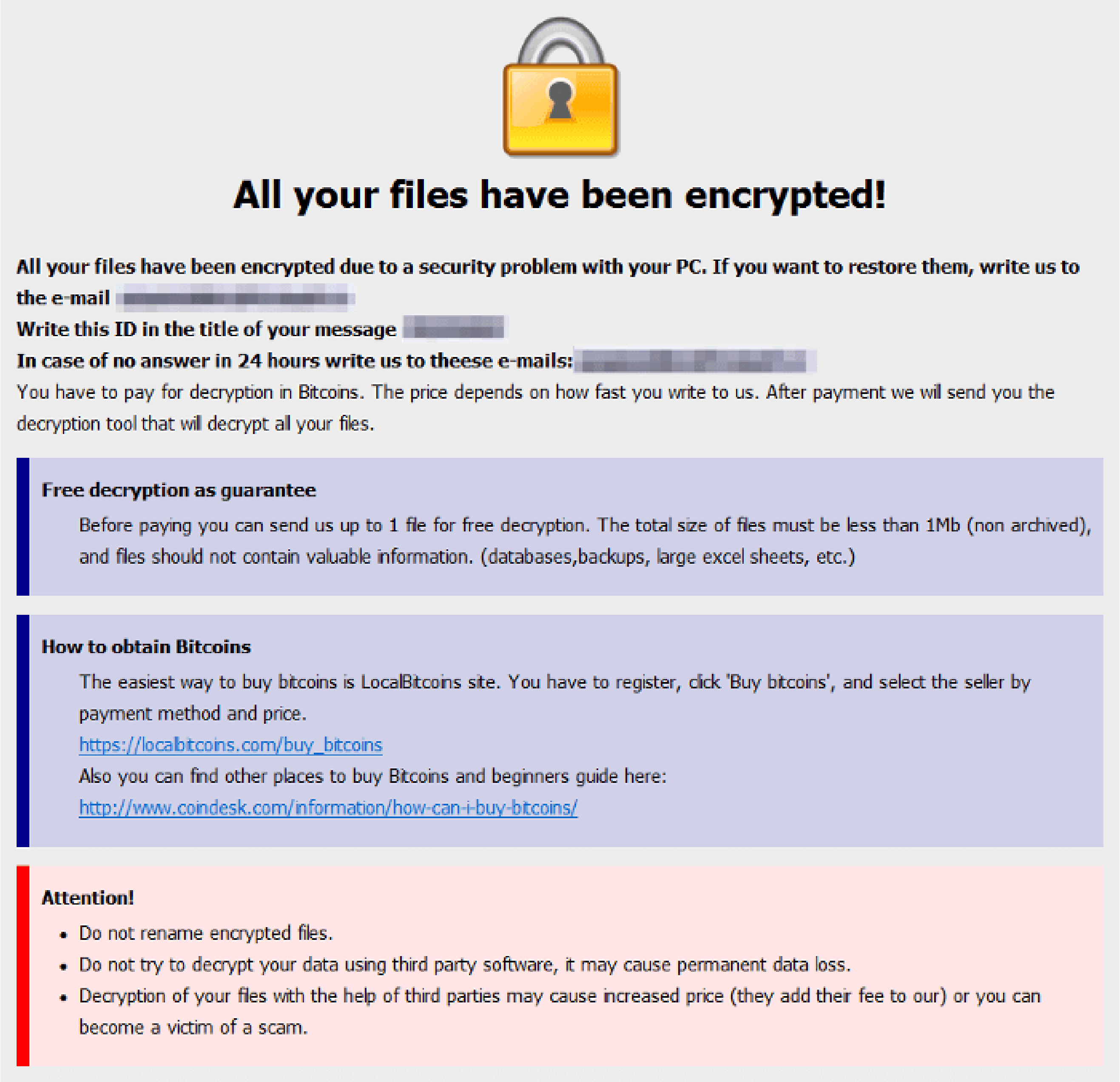
Dharma (also known as Crysis) attacks seem to run to a simple, cookie cutter script with attackers breaking in and then downloading the things they need to execute an attack from the internet as if reading from a todo list: exploits to escalate their privileges, admin or troubleshooting tools to tackle security software, and finally the ransomware itself.

Although simple, the attacks show more variability, and occur at a much greater frequency, than either SamSam or BitPaymer attacks, which may indicate that Dharma is used by multiple groups.

Once the attacker is inside the victim's network they place the ransomware on one or more of a victim's servers manually. Consequently, attacks are often limited in scope, affecting just a few servers.

Most Dharma attacks seem to have affected small businesses of up to 150 users, although it's not known if this is down to deliberate targeting or simply a side-effect of something else.

Ransom demands are made over email, using an address specified in the ransom note, away from prying eyes.



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail [redacted]
Write this ID in the title of your message [redacted]
In case of no answer in 24 hours write us to theese e-mails: [redacted]
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

SamSam

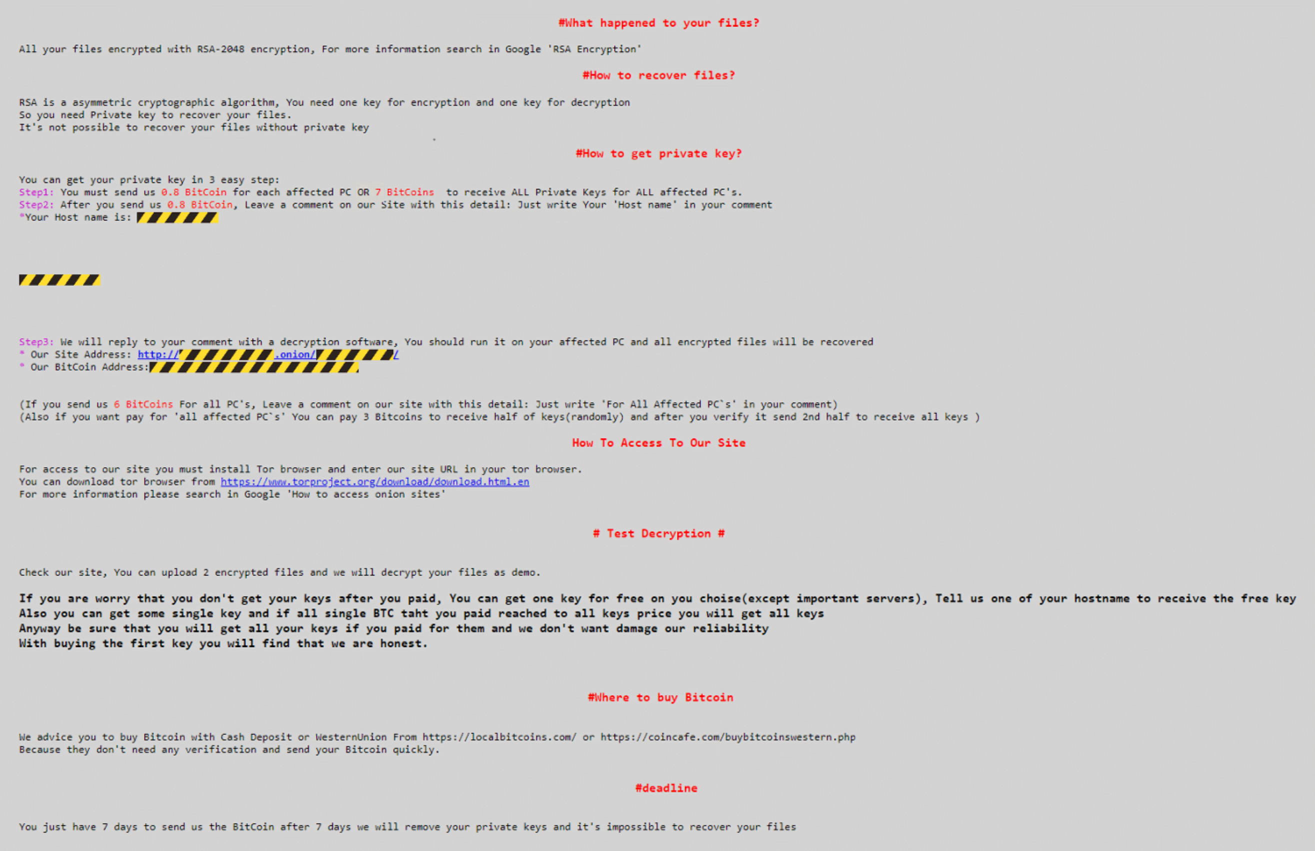
SamSam malware first appeared in December 2015 and since then more than $6 million has been deposited into SamSam Bitcoin wallets.

The pattern of attacks and the evolution of the SamSam malware suggests that it’s the work of one person or a small group. Attacks are infrequent (around one a day) compared to other kinds of ransomware, but are devastating.

After breaking in via RDP, the attacker attempts to escalate their privileges to the level of Domain Admin so that they can deploy SamSam malware across an entire network, just like a sysadmin deploying regular software.

The attacker seems to wait until victims are likely to be asleep before unleashing the malware on every infected machine simultaneously, giving the victim little time to react or to prioritise, and potentially crippling their network.

A ransom note demands payment of about $50,000 in bitcoins and directs the victims to a dark web site (a Tor hidden service).



```
                                   #What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

                                     #How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

                                    #How to get private key?

You can get your private key in 3 easy step:
Step1: You must send us 0.8 BitCoin for each affected PC OR 7 BitCoins  to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.8 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: [redacted]


[redacted]


Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
* Our Site Address: http://[redacted].onion/[redacted]/
* Our BitCoin Address:[redacted]


(If you send us 6 BitCoins For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC`s' in your comment)
(Also if you want pay for 'all affected PC`s' You can pay 3 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys )

                                    How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'


                                       # Test Decryption #


Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), Tell us one of your hostname to receive the free key
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.



                                       #Where to buy Bitcoin


We advice you to buy Bitcoin with Cash Deposit or WesternUnion From https://localbitcoins.com/ or https://coincafe.com/buybitcoinswestern.php
Because they don't need any verification and send your Bitcoin quickly.


                                            #deadline


You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files
```

Each victim has their own page on the site where they can ask the attacker questions and receive instructions on how to decrypt their files.

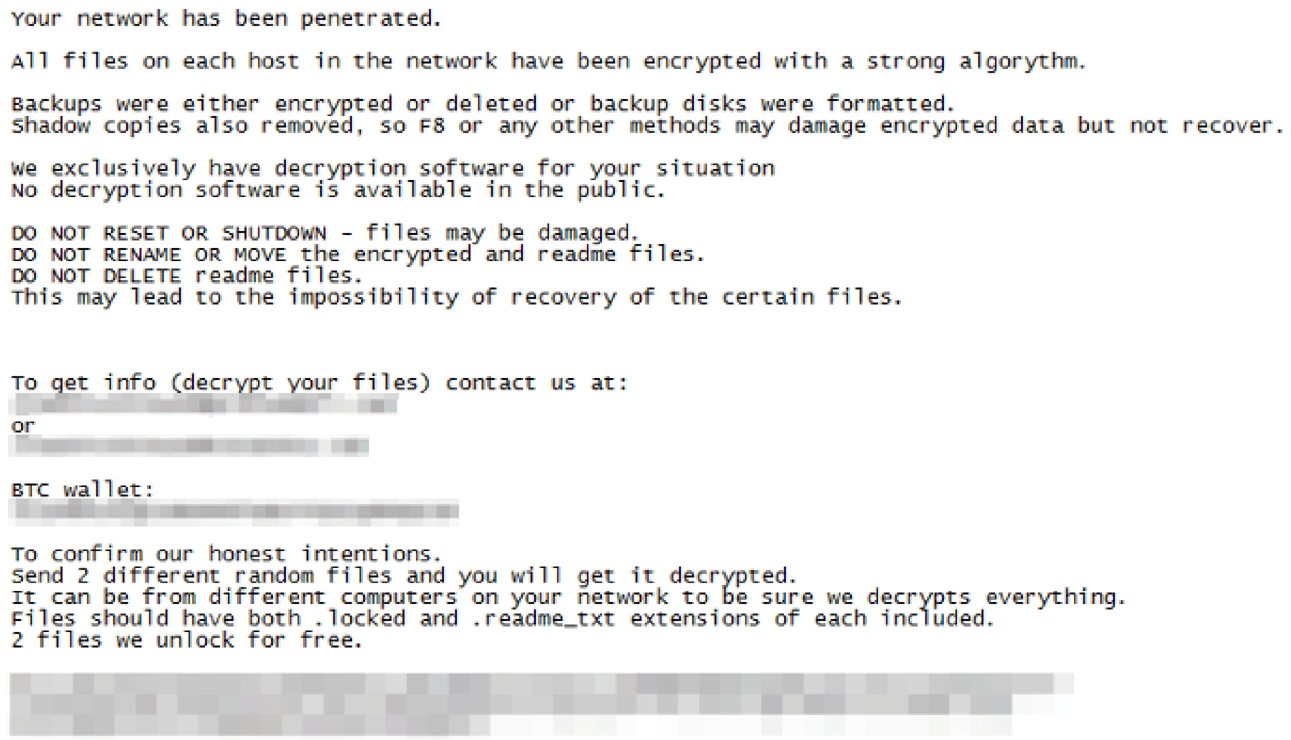
To find out more about SamSam, read Sophos’s extensive new research, SamSam: The (almost) six million dollar ransomware.

BitPaymer

The most mysterious and sophisticated malware on our list is BitPaymer. Little is known about this elusive malware, or how it's deployed (you can read about one of the tricks it uses to hide itself in our article, How BitPaymer ransomware covers its tracks).

What seems certain is that this 'high end' ransomware has raised a lot of money for its creators. Six-figure ransom demands as high as $500,000 have been reported and analysis of known BitPaymer Bitcoin addresses shows that it's raised at least $1 million in the last month alone.

Ransom notes contain email addresses at secure email providers but the method for agreeing payment varies: some simply include a Bitcoin address while others list a dark web URL instead, like SamSam. In some attacks the victims have also been threatened with doxing.



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at:
[redacted]
or
[redacted]

BTC wallet:
[redacted]

To confirm our honest intentions.
Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure we decrypts everything.
Files should have both .locked and .readme_txt extensions of each included.
2 files we unlock for free.

[redacted]
```

What to do?

Targeted attacks may be relatively sophisticated but the criminals behind them aren't looking for a challenge, they're looking for vulnerable organisations. The best way to get yourself off an attacker's hit list is by getting the basics right: lock down RDP and follow a strict patching protocol for your operating systems and the applications that run on them.

If an attacker does get on your network then make sure they're met with layers of overlapping defences, a well segmented network, user rights assigned according to need rather than convenience, and be sure that your backups are offline and out of their reach.

We recently published a detailed guide on how to defend yourself against SamSam ransomware, that includes specifics on how to lock down RDP, suggestions on how to organise your user accounts and more. The advice and approach in it are applicable to all the targeted ransomware mentioned in this article.