Conti ransomware affiliate goes rogue, leaks “gang data”

nakedsecurity.sophos.com/2021/08/06/conti-ransomware-affiliate-goes-rogue-leaks-company-data/

By Paul Ducklin

06 Aug 2021

If you like a touch of irony in your cybersecurity news, then this has been the week for it.

Yesterday, we wrote about an exploitable security hole…

…inside a hacking tool that helps you exploit security holes.

Today, we’re writing about a ransomware-related data breach that leaked organisational information…

…from inside a ransomware group.

And if that’s not enough to bring a wry smile to your lips, then there’s more.

Today’s data breach includes a bunch of hacking tools that ransomware crooks love to use…

…including a buggy and exploitable pirated version of the very attack tool that we wrote about yesterday!

Simply told

The story, it seems, is simply told.

As you already know, many of today’s ransomware attacks aren’t conducted by the core criminals who actually write the malware code.

The core crooks like to keep out of the limelight by recruiting “affiliates” to handle the actual network intrusions.

(These cybergangs often use regular business vocabulary, even referring to their victims as “customers” and describing their extortion attempts as “negotiations”.)

In theory, affiliates can get really rich, because they typically get paid 70% of any ransom that gets extorted – and individual ransoms can run into millions of dollars these days.

And in practice, the core criminals – the ones who write the malware, operate the “affiliate system”, and collect the Bitcoin blackmail payments – can get super-rich, because they get 30% of everything.

However, according to The Record, which published a screenshot of a post in a cybercrime forum by a user discussing the Conti ransomware crew:

> Yes, of course they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays.

The implication, clearly, is that affiliates in the Conti ransomware crew are not being paid 70% of the actual ransom amount, but 70% of an imaginary but lower number.

The critical user followed up the post above with one linking to an 81MByte archive file named `Мануали для работяг и софт.rar` (*Operating manuals and software*).

Dishonour amongst thieves, it seems.

No vital secrets

Ultimately, the data leaked by the disaffected affiliate doesn’t really amount to much.

The criminals at the core of so-called ransomware-as-a-service groups keep the source code, the decryption keys and the blackmail payment details to themselves.

So, this leak won’t help any ransomware victims to decrypt scrambled files without paying.

In fact, if you are minded to get a copy of the leaked files for yourself to see what this is all about, in the hope that it might give you some tricks and tips for defending against ransomware that you didn’t already know…

…please be careful, because the files include numerous hacking and system exploitation tools, conveniently collected in one place, together with instructions and advice (mostly written in Russian).

Think of it as a dump of the Conti gang's community knowledgebase, with plenty of risky software thrown in.

If you're a Sophos customer, you can use the following detection names to search your own logs for the tools included in the breach:

```
ATK/PowSploit-E    <-- Kerberoast, used for attacking Active Directory logons

ATK/Cobalt-*       <-- "Cobalt Strike", a complete botnet system for "threat
emulation"
ATK/Shellcode-*    <-- Exploit injectors included in Cobalt Strike
Troj/Agent-*       <-- Various backdoor "zombie" modules include in Cobalt Strike

GMER               <-- Popular detector/remover for rootkits (and security software)
Harmony Loader     <-- Toolkit for fileless execution of programs via C-Sharp
PC Hunter          <-- Low-level security spelunking tool
PowerTool          <-- Another low-level security spelunking tool
Stas'M Router Scan <-- Scans and looks for holes in routers, Wi-Fi access points and
more
```

Documents leaked in the breach offer basic advice on numerous topics, including:

- Dumping password hashes.
- Turning Defender off by hand.
- Installing and using Metasploit.
- Scanning networks for backup devices.
- Opening backdoors into a compromised network.
- Using popular exploits.
- Elevating privilege.
- Listing users.

There's also a small collection of tools for disabling or uninstalling various anti-virus programs.

There's even a dramatically named batch file called `DIEsophos.bat` in the mix. (It's hard to know whether to be proud or angry that the criminals felt strongly enough to use CAPITAL LETTERS in their filename.)

According to our Managed Threat Response (MTR) team, if Sophos customers have Tamper Protection enabled, then the anti-Sophos measures in the leaked documents won't work, even if the attacker is already an Admin and can get into Windows Safe Mode. If you aren't using Tamper Protection, we recommend you turn it on now.

What to do?

We're going to repeat the advice that we gave yesterday in the wake of the Cobalt Strike bug:

> If your security tools come up with a “Cobalt Strike” alert, or reports that relate to any of the techniques and tools that we mentioned above, we recommend that you investigate immediately, even if your cybersecurity software tells you that it automatically blocked and removed the rogue software that caused the alert.
>
> That’s because intrusions of this sort mean that someone was trying to establish a beachhead inside your network, perhaps for a ransomware attack, perhaps for a data heist, perhaps for both, or perhaps for a range of other criminal activity, too…
>
> …and if they got in once, it’s reasonable to assume that if you don’t find and close the door on them, they (or someone else) will get in again, because that’s quite literally what cybercrooks do for a living.

The good news here is that the leaked data doesn’t really tell us anything we didn’t already know, or introduce any new tools or techniques that the typical cybercrook didn’t already know about, either.

The bad news here, of course, is that the leaked data doesn’t really tell us anything we didn’t already know.

So if you were hoping that the leak was going to be juicy enough to include free decryption keys, or personally identifiable data that might help law enforcement to track down some of these criminals…

…not this time, we’re sorry to say.