The double extortion business: Conti Ransomware Gang finds new avenues of negotiation

darktrace.com/en/blog/the-double-extortion-business-conti-ransomware-gang-finds-new-avenues-of-negotiation/

Justin Fier, Director of Cyber Intelligence & Analytics | Wednesday December 8, 2021

In a previous blog, we outlined how the Ryuk ransomware strain developed by Russian hacking group 'Wizard Spider' has fallen into the hands of small-time cyber criminals.

Wizard Spider – who allegedly operate with support from the Russian government and remain under investigation by the FBI and Interpol – adopted Ryuk ransomware's successor 'Conti' in 2020. Conti affects all Windows operating systems and has been involved in more than 400 incidents. Wizard Spider were soon rebranded in cyber press as the 'Conti Ransomware Gang', though the group does not necessarily see itself as a 'gang'. It prefers to present itself as a business.

The ransomware bubble

Ransomware has become a multibillion-dollar industry – and the Conti Ransomware Gang reportedly made up 15% of it in 2020. With this scale of income, groups like Conti find themselves adopting some crude imitations of legitimate business practice. This corporate mimicry dictates that their victims be called 'customers', their extortion attempts 'negotiations' and their criminal peers 'affiliates'. They even publish 'press releases' via a dedicated Dark Web site.

The gang's Ransomware-as-a-Service 'business model' consists of employing affiliates, training them in Conti ransomware's deployment and management, and then taking 30% of the profits themselves. With exact profits known only to the malware writers and not the affiliates, however, the percentage Conti takes is often much higher than the 30% they claim.

There may not be checks and regulations in place to address fraud in the cyber underworld, but one business complication which Conti have not been able to escape is that of the disgruntled employee.

Unhappy with the malpractice of their superiors, an underpaid affiliate leaked the Conti Ransomware Gang's training materials and the IP addresses for their Cobalt Strike C2 servers in August 2021, declaring, "they recruit suckers and divide the money among themselves".

Meanwhile, the US Government has also been taking action to try to disrupt the profit margins of groups like the Conti Ransomware Gang, going as far as to impose sanctions on cryptocurrency exchanges seen as facilitating ransomware transactions. However, leaks and legislation have proved far from fatal for Conti.

The reality is that these actions have not lost the Conti Ransomware Gang any of its so-called "customers", and where there are customers there is profit. Any individual or organization entrusting their cyber security to conventional, rules-based measures is in their target market.

Darktrace's AI recently detected a Conti attack conducted along the lines of one of the methods outlined in the August leak. The target organization – a US transportation company – was trialling Darktrace but, without Darktrace's Autonomous Response set in active mode, the attack was allowed to go ahead. In examining how it progressed, however, it should become clear not only how threatening double extortion ransomware attacks like this one can be, but also how effectively they can be stopped by Darktrace at each stage of the attack.


Figure 1: Timeline of the attack

Conti Ransomware Gang diversifies the ransomware playbook

A single uninstalled Microsoft patch had left the target organization with dangerous ProxyShell vulnerabilities. Conti exploited these vulnerabilities, quickly gaining the rights to remotely execute Exchange PowerShell commands on the company's server and steadily broadened its presence within the digital environment. This is a relatively new approach for the Conti Ransomware Gang, who previously relied upon phishing attacks and firewall exploits. By diversifying its approach, it stays ahead of patches and intelligence.

Two weeks after the initial breach, C2 connections were made to an unusual endpoint located in Finland using an SSL client which appeared innocuous but was 100% rare for the organization. Had Autonomous Response been set in active mode, Darktrace would have shut the connections down at this very early stage.

The IP address of this suspicious endpoint has since been identified as a Conti IoC (Indicator of Compromise), allowing it to be incorporated into rules-based security solutions. This would have done little good for the company in question, however, which was breached weeks before this intelligence was made available.

As Conti continued to conduct internal reconnaissance and move laterally through the company's digital environment, Darktrace detected further unusual activity. The suspicious Finnish endpoint then employed new 'Living off the Land' techniques, installing the usually legitimate tools AnyDesk and Cobalt Strike onto various parts of the environment.

A series of SSL connections were made to AnyDesk endpoints and external hosts, one of which lasted 95 hours, indicating an active remote session conducted by one of Conti's affiliates. At this stage, Darktrace had 10 distinct reasons to suspect an imminent attack.

Conti News: Closing the deal with double extortion ransomware

Double extortion has become the Conti Ransomware Gang's new favourite sales tactic. If you refuse to pay its ransom, Conti will not only take your most important files from you, but also exfiltrate and publish them using its dedicated 'Conti News' website, or sell them directly to your competitors.

Having expanded their reach across the transport company's network, the Conti affiliate began rapidly exfiltrating large quantities of company data to Conti's preferred cloud storage site, MEGA. Over four days, more than 3TB of data was uploaded, and then encrypted.

To avoid detection by a human security team, encryption was launched at close to midnight – Conti's 'business' does not respect business hours. When the company's security team returned to work the next day, they were met with a ransom note.

> All of your files are currently encrypted by CONTI strain. ... .As you know (if you don't just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. .. If you try to use any additional recovery software — the files might be damaged, so if you are willing to try — try it on the data of the lowest value... . To make sure that we REALLY CAN get your data back — we offer you to decrypt 2 random files completely free of charge.
>
> YOU SHOULD BE AWARE ! Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

This attack was able to progress because Darktrace was only being trialed at this stage and was therefore allowed to detect threats but not to take action against them. With Autonomous Response employed in active mode, this ransomware attack would have ended in the very early stages, when Darktrace detected its first suspicious connections.

Nonetheless, the Cyber AI Analyst was able to investigate and connect the dots of the attack automatically, making the organization's remediation efforts drastically quicker and easier than they would have been without even this partial Darktrace deployment.


Figure 2: Cyber AI Analyst generated this incident report following the initiation of data exfiltration

How the Conti Ransomware Gang evades cyber intelligence

Security systems that rely on human intelligence to detect threats fit Conti's ideal customer profile perfectly. By adapting and diversifying their approach, moving from Ryuk to Conti, and from spear phishing and firewall exploits to this new ProxyShell approach, Conti stay ahead of regulations and hold on to their vulnerable customer base.

Even if the Conti Ransomware Gang is brought down by leaks or legislation, other groups will rise to fill the gap in the market, eager for their own cut of the illicit gains. If these groups are to be truly stopped, they must be made unprofitable.

The US government has tried to do this by imposing fines upon ransom payers, but companies still often consider the losses involved in not recovering their data too great. As I have argued previously, 'to pay or not to pay,' is not the question we should be asking.

If you're deciding whether to pay or not to pay, you're already too far down the line. Darktrace stops groups like Conti at the first encounter. As this case has shown, Darktrace's Self-Learning AI is able to identify threats weeks before human analysts and threat intelligence can do the same, and neutralize them at every stage of an attack with Autonomous Response.

Thanks to Darktrace analyst Sam Lister for his insights on the above threat find.

Darktrace for Ransomware: Learn more

Technical details

IoCs

IoC	Comment

70.39.126[.]171	IP address of external endpoint used to gain foothold on autodiscover server
135.181.10[.]218	IP address of external endpoint which autodiscover contacted (presumably) as a result of an external endpoint issuing a PowerShell command on the server
64.120.44[.]116	IP address of external endpoint which potentially issued PowerShell commands to autodiscover server
92.223.88[.]7 64.31.35[.]242 203.10.96[.]34 103.253.43[.]112	IP addresses of endpoints to which AnyDesk connections were made
Port 7070	AnyDesk port
d1n2x5h0loustn[.]cloudfront[.]net	Hostname of Cobalt Strike command and control servers
13.226.235[.]221 13.225.141[.]128 13.225.141[.]32 13.226.235[.]11	IPs of Cobalt Strike commant and control servers
rclone/v1.53.3	User-agent string used in HTTP data exfiltration
.UGKMP	File extension appended to encrypted files

Darktrace model detections:

- Device / Long Agent Connection to New Endpoint
- Device / ICMP Address Scan
- Anomalous Connection / SMB Enumeration
- Anomalous Server Activity / Outgoing from Server
- Compromise / Beacon to Young Endpoint
- Anomalous Server Activity / Rare External from Server
- Compromise / Fast Beaconing to DGA
- Compromise / SSL or HTTP Beacon
- Compromise / Sustained SSL or HTTP Increase
- Compromise / Beacon for 4 Days
- Anomalous Connection / Multiple HTTP POSTs to Rare Hostname
- Unusual Activity / Enhanced Unusual External Data Transfer
- Anomalous Connection / Data Sent to Rare Domain
- Anomalous Connection / Uncommon 1 GiB Outbound
- Compliance / SMB Drive Write
- Anomalous File / Internal / Additional Extension Appended to SMB File
- Anomalous Connection / Suspicious Read Write Ratio

- Anomalous Connection / Suspicious Read Write Ratio and Unusual SMB
- Anomalous Connection / Sustained MIME Type Conversion
- Unusual Activity / Anomalous SMB Move & Write
- Unusual Activity / Unusual Internal Data Volume as Client or Server
- Device / Suspicious File Writes to Multiple Hidden SMB Shares
- Compromise / Ransomware / Suspicious SMB Activity
- Anomalous File / Internal / Unusual SMB Script Write
- Anomalous File / Internal / Masqueraded Executable SMB Write
- Device / SMB Lateral Movement
- Device / Multiple Lateral Movement Model Breaches

MITRE ATT&CK techniques observed:

Initial Access	T1190 – Exploit Public-Facing Applications
Execution	T1059.001 — Command and Scripting Interpreter: PowerShell
Command and Control	T1573 — Encrypted Channel T1219 — Remote Access Software
Discovery	T1018 — Remote System Discovery T1083 — File and Directory Discovery
Exfiltration	T1567.002 — Exfiltration Over Web Service: Exfiltration to Cloud Storage
Lateral Movement	T1021.002 — Remote Services: SMB/Windows Admin Shares
Impact	T1486 — Data Encrypted for Impact

Justin Fier

Justin is one of the US's leading cyber intelligence experts, and holds the position of VP, Tactical Risk and Response at Darktrace. His insights on cyber security and artificial intelligence have been widely reported in leading media outlets, including the Wall Street Journal, CNN, The Washington Post, and VICELAND. With over 10 years' experience in cyber defense, Justin has supported various elements in the US intelligence community, holding mission-critical security roles with Lockheed Martin, Northrop Grumman Mission Systems and Abraxas. Justin is also a highly-skilled technical specialist, and works with Darktrace's strategic global customers on threat analysis, defensive cyber operations, protecting IoT, and machine learning.