MUST WATCH: Boston Dynamics bipedal robots complete parkour obstacle course

This ransomware has returned with new techniques to make attacks more effective

LockBit ransomware has been around since 2019, but those behind it are adding new features and aggressively advertising to attract new cyber criminal affiliates.

By Danny Palmer | August 18, 2021 -- 12:13 GMT (05:13 PDT) | Topic: Security

Ransomware: Do these three things to help protect your network from attacks

WATCH NOW ()

There's been a rise in cyber attacks using a form of ransomware (h

article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/) that first appeared almost two years ago. But despite being relatively old, it's still proving successful for cyber criminals.

Cybersecurity researchers at Trend Micro have detailed an increase in LockBit ransomware campaigns (https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html) since the start of July. This ransomware-as-a-service first appeared in September 2019 and has been relatively successful, but has seen a surge in activity this summer.

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                 Press ENTER to continue
```

(https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/)

Ransomware: An executive guide to one of the biggest menaces on the web (https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/)

Everything you need to know about ransomware: how it started, why it's booming, how to protect against it, and what to do if your PC is infected.

Read More (https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/)

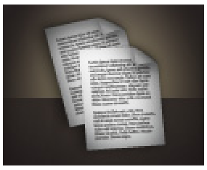
In adverts on underground forums, LockBit's authors (https://www.zdnet.com/article/a-deep-dive-into-the-operations-of-the-lockbit-ransomware-group/) claim that LockBit 2.0 is one of the fastest file-encrypting ransomware variants in the market today. And those claims have proven interesting to cyber criminals seeking to make money from ransomware.

Trend Micro researchers have seen a number of LockBit ransomware campaigns in recent weeks, predominantly targeting organisations in Chile, but also the UK, Italy and Taiwan.

While LockBit has remained under the radar for much of this year, it hit the headlines with an attack against professional services firm Accenture (https://www.zdnet.com/article/accenture-says-lockbit-ransomware-attack-caused-no-impact-on-operations-or-clients/). LockBit also appears to have benefited from the apparent disappearance of ransomware gangs including REvil and Darkside (https://www.zdnet.com/article/revil-websites-down-after-governments-pressured-to-take-action-following-kaseya-attack/), with a significant number of affiliates of those operators turning towards LockBit (https://www.zdnet.com/article/one-big-ransomware-threat-just-disappeared-now-another-one-has-jumped-up-to-fill-the-gap/) as their new means of performing ransomware attacks.

The attackers often gain entry to networks using compromised Remote Desktop Protocol (RDP) or VPN accounts (https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/) which have been leaked or stolen; alternatively, LockBit attacks sometimes attempt to recruit insiders to help gain access through legitimate login credentials.

SEE: A winning strategy for cybersecurity (http://www.zdnet.com/topic/a-winning-strategy-for-cybersecurity/?ftag=CMG-01-10aaa1b) (ZDNet special report)



LockBit has also gained success by following in the footsteps of prominent ransomware groups using certain tactics, techniques and procedures (TTPs) during attacks. For example, LockBit now uses Ryuk's Wake-on-LAN feature (https://www.zdnet.com/article/this-dangerous-ransomware-is-using-a-new-trick-to-encrypt-your-network/), sending packets to wake offline devices in order to help move laterally around networks and compromise as many machines as possible.

LockBit also uses a tool previously deployed by Egregor ransomware (https://www.zdnet.com/article/ransomware-this-new-variant-could-be-the-next-big-malware-threat-to-your-business/), using printers on the network to print out ransom notes.

"They were heavily influenced by the Maze ransomware gang and when they shut down, they appear to have shifted their focus to Ryuk and Egregor ransomware gangs TTPs," Jon Clay, VP of threat intelligence at Trend Micro, told ZDNet.

"What we can take away from this is many malicious actor gangs likely follow the news of how successful other gangs are and look to model their TTPs themselves. Ransomware h me in order to continue to be successful for its creators," he added.

Like many of the most disruptive ransomware variants, LockBit also adds a double extortion element (https://www.zdnet.com/article/ransomware-theres-been-a-big-rise-in-double-extortion-attacks-as-gangs-try-out-new-tricks/) to attacks, stealing data from the victim and threatening to leak it if the ransom isn't paid within a set period.

"The LockBit gang has been around for a while now and continue to update their TTPs in order to have successful attack campaigns," said Clay.

It's expected that LockBit ransomware attacks will continue to be a cybersecurity threat for some time, particularly given that the group is actively advertising for additional affiliates. But while ransomware groups are aggressively persistent, there are actions which information security teams can take to help protect networks from attack.

This includes applying the latest security patches and updates (https://www.zdnet.com/article/this-one-change-could-protect-your-systems-from-attack-so-why-dont-more-companies-do-it/) to operating systems and software, so cyber criminals can't exploit known vulnerabilities to help launch attacks. Organisations should also apply multi-factor authentication across the network (https://www.zdnet.com/article/multi-factor-authentication-use-it-for-all-the-people-that-access-your-network-all-the-time/), making it harder for cyber criminals to use stolen credentials to help facilitate attacks.

MORE ON CYBERSECURITY

- **Ransomware: Now attackers are exploiting Windows PrintNightmare vulnerabilities** (https://www.zdnet.com/article/ransomware-now-attackers-are-exploiting-windows-printnightmare-vulnerabilities/)
- **This major ransomware attack was foiled at the last minute. Here's how they spotted it** (https://www.zdnet.com/article/this-ransomware-attack-was-foiled-at-the-last-minute-heres-how-they-spotted-it/)
- **New DOJ task force to take on ransomware, says report** (https://www.cnet.com/tech/services-and-software/new-doj-task-force-to-reportedly-take-on-ransomware/)
- **Ransomware: This new free tool lets you test if your cybersecurity is strong enough to stop an attack** (https://www.zdnet.com/article/ransomware-this-new-free-tool-lets-you-test-if-your-cybersecurity-is-strong-enough-to-stop-an-attack/)
- **Have we reached peak ransomware? How the internet's biggest security problem has grown and what happens next** (https://www.zdnet.com/article/have-we-reached-peak-ransomware-how-the-internets-biggest-security-problem-has-grown-and-what-happens-next/)