GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

February 2022

Preparing for the Possibility of Russian Ransomware Attacks

On Feb 25, 2022, one of the top 10 ransomware threat actor groups, Conti, issued a statement announcing its "full support" of the Russian government and threatening "to use all our possible resources to strike back at critical infrastructures of an enemy" who "organize[s] a cyberattack or any war activities" against Russia. Conti followed up with a second statement reiterating its threat but clarifying that "we do not ally with any government."

These threats come on the heels of a warning issued earlier this week by the U.S. Department of Homeland Security that companies should be on alert for cyber-attacks as the United States and allied nations increase sanctions on Russia. Such attacks have already occurred against the Ukrainian government and banking institutions in the past few weeks. The Department of Homeland Security has stated that it has no specific or credible threats against the United States, but warns companies to prepare for the possibility.

With the ever-evolving crisis in Ukraine, companies should be aware of these warnings and be increasingly vigilant against the risk of cybersecurity attacks, including ransomware and distributed-denial-of-service attacks (DDOS), particularly for companies engaged in critical infrastructure or doing business with Ukraine.

Companies attempting to prepare and reduce risk may consider taking the following steps:

- Ensure a recent copy of back-ups of key systems is stored offline or otherwise segregated from the Company's network.
- Test back-ups to ensure they are viable and can be restored quickly.
- Identify workarounds for key business functions, including manual workarounds, to enable the Company to operate while it addresses a cyber-attack.
- Require multi-factor authentication for remote access and privileged and administrative access to systems.
- Consider changing passwords as Conti has been known to reuse credentials compromised in other incidents, especially those accounts with escalated privileges.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities, including Log4J.
- Disable all ports and protocols that are not essential for business purposes.
- Ensure that IT personnel have reviewed and implemented strong controls for cloud computing.
- Conduct vulnerability scanning and risk assessments.
- Implement monitoring tools, like endpoint detection and response (EDR), to identify intrusions or anomalous activity.
- Enable logging in order to better investigate issues or events and ensure logging cannot be easily disabled by an attacker.
- Confirm that the organization's entire network is protected by antivirus/anti-malware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations and closely review access controls for that traffic.
- Identify members of an incident response team and assign roles to each member to respond to an incident, including legal, technology, communications, business continuity, and regulatory reporting.
- Identify key stakeholders who may need to be informed right away of an incident, especially any third parties' whose systems could be accessed by a threat actor moving laterally from your organization.
- Ensure key personnel are available and have exchanged personal contact information so they can easily connect in the event of an incident.
- Identify external resources (legal, forensics, disaster recovery) to engage immediately in an incident.
- If possible, test your team and response plan via a tabletop exercise to ensure that everyone understands what will be expected of them in a cyber incident.

Below is a non-exhaustive list of indicators of compromise (IOCs) associated with Conti that may indicate the risk of an attack by Conti or another ransomware group.

- Delete.me
- System32.exe

- Nosleep!.exe
- Process hacker 2
- Rclone
- Data.dll
- Gvrty.exe
- AnyDesk
- Splashtop
- Aterra
- Cobalt Strike
- Mimikatz

Author

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com

Greenberg Traurig's 24/7 Data Breach Hotline: 855.3BREACH