Why & How To Protect Against Ransomware

With many employees working remotely during the COVID-19 response, their employers' networks and information systems are exposed to a much higher risk of hacking and ransomware. **Governmental entities are a significant target for cyber criminals – and ransomware is their most common type of cyber attack.** Cyber criminals usually deploy ransomware through phishing emails and by breaching poorly secured Remote Desktop Protocol systems (RDPs). **RDPs are very convenient for giving employees access to their work computer from home, but they can become real liabilities if they are not set up with sufficient security elements.**

Ransomware and Preventing Cyber Breaches* (linked below under "Documents") goes into some detail about how this happens and how to prevent it. Among other things, it explains how cyber criminals

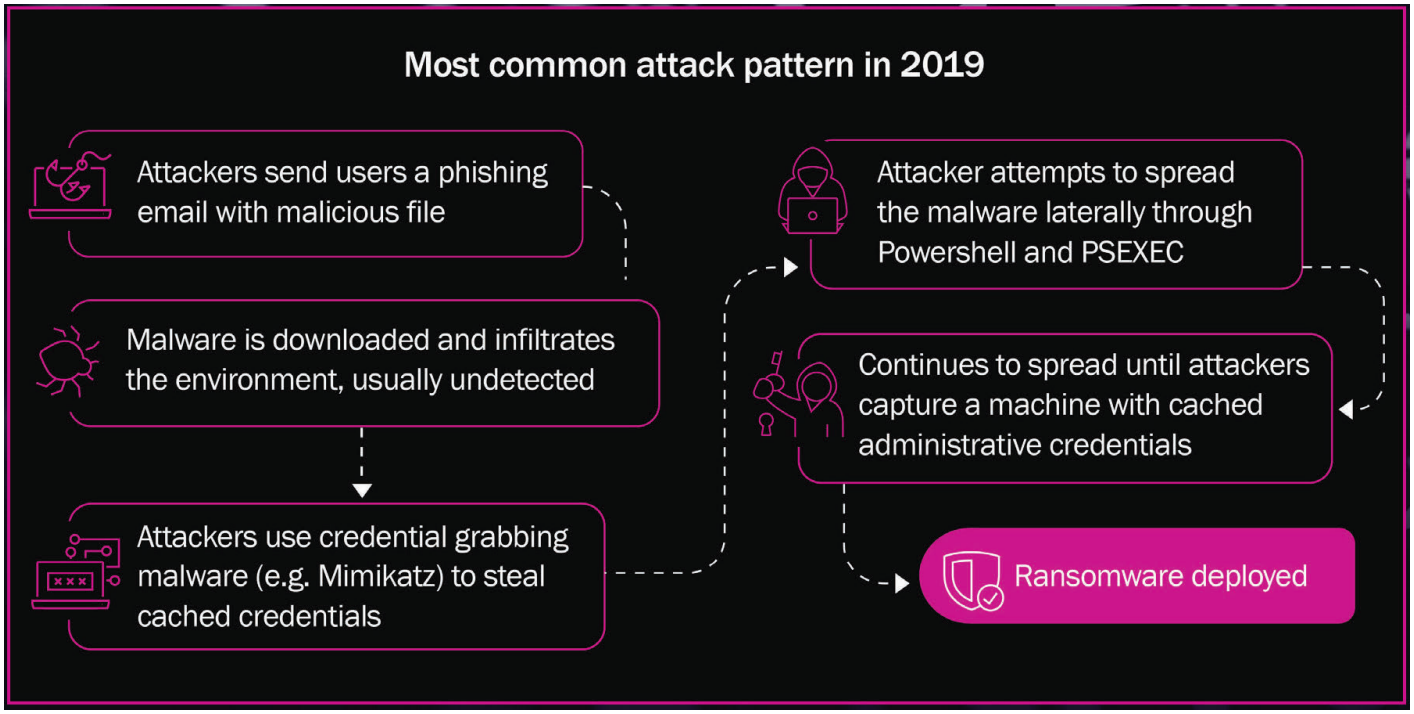
1. trick users into handing over secure information, and
2. gain access to ("breach") Remote Desktop Protocol (RDP) systems that are not set up with proper security.

To maintain system security when working remotely, PACIF's partner for cybersecurity coverage* recommends that employees take additional measures to reduce the vulnerability of your IT infrastructure. They specify **three important forms of protection**:

- Train employees to recognize phishing attempts and to never click the links. Basic courses are available for PACIF members through the PACIF Online University.
- Ensure that employees can access their computer using a virtual private network. Multifactor authentication is a best practice and is highly encouraged.
- "Whitelist" the IP addresses that are allowed to connect via the RDP. Every remote user – especially third parties – must set up unique credentials for access.

VLCT PACIF's recommendation is that you **discuss these and other computer network security elements with your IT system vendor(s) to make sure your remote system operations are at least as secure as they would be when working from the office**.

* Published in early 2020 by Beazley Insurance Company, Inc., a leading cyber liability insurer and PACIF's reinsurer for cyber liability coverage, this document is based on computer hacking and ransomware claims filed with Beazley in 2019.



Documents:

Ransomware and Preventing Cyber Breaches – from the Beazley Insurance Company [1]

Links:

PACIF Advice on Cybersecurity – guidance [2]
Cybersecurity – webpage by VLCT Municipal Assistance Center [3]
Cybersecurity Handouts for Employees – infographics [4]
Remote Work Cybersecurity – webinar on 4/15/20 by Sherri Davidoff of LMG Security [5]
How To Evaluate Your Information Technology Systems – article from July-August 2020 VLCT News [6]
It's All About Protecting The Data – article from July-August 2020 VLCT News [7]
Email Scams are a Real Threat to Vermont Municipalities – article from July-August 2020 VLCT News [8]

Resource Category:

- Guidance

Links

[1] https://www.vlct.org/sites/default/files/documents/Resource/Cyber-breach-briefing-2020.pdf
[2] http://www.vlct.org/node/14856
[3] http://www.vlct.org/node/11268
[4] http://www.vlct.org/node/15192
[5] http://www.vlct.org/node/15417
[6] http://www.vlct.org/node/15502
[7] http://www.vlct.org/node/15498
[8] http://www.vlct.org/node/15501