

MAY 16, 2017

## Cybersecurity Memo

# “WannaCry” and Ransomware

On May 12, 2017, a new ransomware program was discovered known as WannaCry, WCry, or Wanna Decryptor. As of May 16, there are over 374,000 unique addresses infected – and growing every minute.

WannaCry attacks by encrypting and holding data for ransom, currently set at 0.1781 bitcoins (approximately \$300 USD). According to the FBI Cyber Division, WannaCry is primarily attacking enterprise systems through two known avenues: Remote Desktop Protocol (RDP) and Windows SMB (or CIFS). There are also reports of infections received through phishing emails.

**Vantage Point will scan your network for ransomware for free. Call us today.**

### What is ransomware?

Ransomware is a form of malware designed to hold a system’s data (anything you save on your computer or server) for ransom. How does it do this? Most commonly, ransomware encrypts the information on your system and prevents you from accessing it until the ransom is paid.

The attackers then demand payment in order to retrieve the data – often under threat of deleting it forever. (That payment is usually requested via bitcoins, a form of crypto currency which is difficult to track.) After payment is made the attacker will claim to send a key for decrypting the system’s data.

### How can I protect my data?

Always be aware of suspicious websites, emails, or messages. When updating Windows systems, allow all security updates. If you use SMB, ensure you receive security updates from Microsoft; if not, you may disable it.

Additional Steps to prevent infections:

- Block SMB and RDP from leaving or entering you network
- Update Windows systems
- Don’t open suspicious emails

### What should I do if I’m infected?

Paying ransom is unlikely to get your data back. In fact, those who do pay ransom may be specifically targeted again in different campaigns. It is also common, if ransom is paid, for the attackers to ask for more than the original ransom.

What to do if you are infected:

- Remove the infected system from the network immediately



- Turn the system off
- Isolate your backups by taking them offline

#### Additional resources and more information:

- [FBI Flash Warning](#)
- [How to Protect Your Networks from Ransomware](#)
- [Windows SMB Security Bulletin](#)

**Vantage Point can scan you for infection immediately.**  
If you are worried about vulnerability to WannaCry or other malware in the future, contact our team of experts today.

#### **Andy Deinert**

NETWORK & SECURITY SERVICES MANAGER

Direct: 605-995-1765

Mobile: 605-999-4924

Andy.Deinert@vantagepnt.com

#### **Gaven Davis**

SENIOR DATA NETWORK CONSULTANT

Direct: 605-995-1794

Mobile: 605-999-6466

Gaven.Davis@vantagepnt.com

#### **Rob Thompson**

SENIOR DATA NETWORK CONSULTANT

Direct: 605-995-1808

Rob.Thompson@vantagepnt.com

#### **Brandon Knutson**

DATA NETWORK SPECIALIST

Direct: 605-995-1795

Mobile: 605-924-6040

Brandon.Knutson@vantagepnt.com

#### **James Taylor**

DATA NETWORK SPECIALIST

Direct: 605-995-1829

James.Taylor@vantagepnt.com

#### **Jon Brown**

SENIOR TECHNOLOGY LEADER

Direct: 605-995-1753

Mobile: 605-999-0922

Jon.Brown@vantagepnt.com

#### **Cody Jenks**

SENIOR DATA NETWORK CONSULTANT

Direct: 605-995-1780

Mobile: 605-999-8515

Cody.Jenks@vantagepnt.com

#### **Justin Haar**

SENIOR IT SECURITY CONSULTANT

Direct: 605-995-1813

Mobile: 605-681-4766

Justin.Haar@vantagepnt.com

#### **Dave Schwalm**

IT SECURITY SPECIALIST

Direct: 605-995-1824

Mobile: 605-695-5618

Dave.Schwalm@vantagepnt.com

**For after-hours support or when your**

**primary contacts are not available**

you can call 605-990-DATA. You can

also email [netmon@vantagepnt.com](mailto:netmon@vantagepnt.com)

to reach the team.