How to Tell if You've Been Hacked

Distributed enterprises, by their very nature, are at a disadvantage when it comes to combating cyberattacks. The fact that they have multiple physical locations means they have a large and often growing attack surface to protect from the ever-increasing number of attacks. Simply not having dedicated cybersecurity resources at every site, and therefore having less robust security at remote locations, puts distributed enterprises at a disadvantage to prevent and mitigate a cyberattack.

Adding to the complexity of growing attack surfaces in distributed enterprises is the human element; employees are often on the front lines when it comes to cyberattacks. In fact, the number one cyber attack scheme in the US in 2021 was phishing or similar attack (54% of all reported attacks).[1] Phishing attacks rely on a person to take an action to collect confidential information, gain access to systems, or receive payments. Being able to recognize suspicious activity can help businesses spot attacks early to minimize damage.

Administrators should train users to look for the following that may indicate an attack:

1. **Ransomware Messages**
   This may be the most obvious indication that you've been hacked and unfortunately it means your data has been encrypted and risks being held hostage unless ransom demands are met. Most victims end up with many days of downtime and additional recovery steps even if they do pay the ransom.

2. **Slow Computer or Battery Draining Quickly**
   If the battery starts draining quickly or your computer suddenly starts crashing or running as fast as a tortoise, you may have been hacked. It could be malicious software running the background slowing down your computer and draining the battery.

Preventing Your Network From Being Hacked

Distributed enterprises are at a cybersecurity disadvantage with many locations and users spread over a large area. In addition to monitoring for the signs of compromise, here are measures every company can take to protect themselves:

- Train employees continuously. As security adversaries find new ways to infiltrate networks, keeping employees trained and up to date will only strengthen your network security.
- Use multi-factor authentication to provide an additional layer of protection of sensitive data.
- Backup your data. If your data is backed up, even if your network is breached, a backup can revert the machine to the data it had on it the day before the attack, minimizing losses.
- Segregate your network for different types of usage and roles. For example, have a guest network that is separate to the main network.
- Keep software up to date and install all software patches expediently to avoid a breach.

3. **Suspicious File Changes**
   If you notice that files have suddenly been deleted for no reason, or document or folder names randomly change, this could be the handy work of a hacker and should be investigated immediately.

4. **Antivirus or Antimalware Programs Are Disabled**
   Has your antivirus or other security software suddenly been turned off? That could be a sign that you've been compromised with malicious software.

5. **Passwords Suddenly Don't Work**
   If you're sure you've entered the correct password and it's still not working, you could be the victim of a hacker who has accessed your account and changed the password to keep you out.

6. **Unwanted Installations**
   Unknown browser toolbars and/or software installed on your computer are not only signs that you've been hacked but they can open malicious files and release malware, disable your antivirus, and cause more unwanted changes.

7. **Other Unusual Activity**

- Internet searches are redirected
- Mouse pointer makes clear movement between programs and makes selections
- Attempted access during odd hours or from odd locations
- Frequent and random popups

Sources

1. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

About Arista Cognitive Unified Edge (CUE)

Arista's CUE solutions help SMBs and distributed enterprises optimize their networks while safeguarding their data and devices. CUE redefines networks with enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network from headquarters to the network edge.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989