Frequently Asked Questions
Recent Cybersecurity Reports
June 8, 2017

What do I need to know about the October spear-phishing emails?

Recent reports indicate that cyber actors impersonated VR Systems and other elections companies. Cyber actors sent an email from a fake account to election officials in an unknown number of districts just days before the 2016 general election. The fraudulent email asked recipients to open an attachment, which would then infect their computer, providing a gateway for more mischief.

Please note:

- We have heard of **no accounts of election officials** who opened the attachment. Most election officials have security systems in place that would have flagged the email before it even reached the intended recipient.

- Neither the EViD pollbook, nor any other VR Systems product, were targets of this attack.

What did the cyber actors hope to achieve? What weakness was the email trying to exploit?

The goal was to trick recipients into opening an attachment that contains malware. The malware would enter that recipient's network. We have no evidence that any customer (or any non-customer) opened the spear-phishing email or that any malware was downloaded.

How do I know if my office received the spear-phishing email?

Because the spear-phishing email did not originate from VR Systems, we do not know how many jurisdictions were potentially impacted. Many election offices report that they never received the email or it was caught by their spam filters before it could reach recipients.

It is our understanding that all jurisdictions, including VR Systems customers, have been notified by law enforcement agencies if they were a target of this spear-phishing attack.

What red flags were raised in the spear-phishing email?

1) It would be highly unusual for VR Systems to issue a communication suggesting a change of software inside a live election timeframe. VR Systems would never make any change to software during a live election unless under unusual circumstances and only after conferring with our customers and the State.

2) Grammatical mistakes and unusual spelling should alert a recipient to a concern.

3) The domain name was incorrect.

What steps should I take to protect my systems?

1) Consult with IT professionals to ensure that all systems are patched and regularly updated.

2) Train all office staff in cybersecurity safety.

3) Engage the services of security experts who can audit your systems and ensure the integrity of your data.

4) If you see something unusual, say something. VR Systems is available by phone any time and any hour, every day of the year and can respond immediately to a concern.

5) Secure all log-in credentials. No staff member from VR Systems will ask you for your log-in and password.

6) Participate in professional cyber-alliances to learn best practices.

For more information, please consult the Domestic Security Alliance Council (https://www.dsac.gov/topics/cyber-resources) which includes a number of links to government security agencies focused on cybercrime prevention.

What is needed to protect all systems?

Cybersecurity is a dynamic environment and it is important to remain vigilant and alert about the latest developments and tools. At VR Systems, we will do our best to communicate protocols and measures to assist our customers in remaining up to date with regard to security.

- Phishing email scams are common. We expect the security environment to become more complex in the coming years and strongly encourage election officials to stay on top of the latest security tools and protocols.

- A combination of technology and well-trained users are needed to prevent security issues.

VR Systems maintains a close relationship and is working in concert with security and law enforcement agencies to maintain robust and current security systems.

Was VR Systems' email hacked in August?

No. In August, a small number of phishing emails were sent to VR Systems. These emails were captured by our security protocols and the threat was neutralized. No VR Systems employee's email was compromised. This prevented the cyber actors from accessing a genuine VR Systems email account.

As such, the cyber actors, as part of their late October spear-phishing attack, resorted to creating a fake account to use in that spear-phishing campaign.

###