Questions and Answers Regarding 2016 Spear-Phishing Emails and Recent Cybersecurity Media Reports

When did VR Systems learn of the October 2016 spear-phishing email?

VR Systems became aware of the spear-phishing email on November 1, 2016 when a customer alerted us to an obviously fraudulent email purporting to come from our company.

How did VR Systems respond to the October 2016 spear-phishing email?

VR Systems took immediate action by notifying customers and law enforcement. We were sent a screenshot of the spear-phishing email by one of our customers at 9:24 am on November 1, 2016 and by 10:14 am that same day, we sent an email to all of our customers alerting them and telling them not to open the email and not to click on the attachment if they received it.

We immediately contacted law enforcement and they responded. This is the protocol that has been established to handle these types of situations. It is our understanding that some customers received the email earlier, but it may have gotten caught in spam or not read immediately and many recognized it as an obvious fake.

Most election officials have security systems in place that would have flagged the email before it even reached the intended recipient. After we notified our customers of the potential threat, most told us that their spam filter caught the email or that they had never received it. We are only aware of a small number of our customers who actually received the fraudulent email and of those, none of them notified us that they clicked on the attachment or were compromised as a result.

After this incident, we hired a leading threat intelligence firm which conducted a byte-by-byte analysis of our systems and found no indications that that our system had been breached as a result of this spear-phishing attack.

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

Was VR Systems' email hacked in August 2016?

No.

Has VR Systems ever received phishing emails?

Yes. In August 2016, 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 emails were compromised. This prevented the cyber actors from accessing a genuine VR Systems email account.

As such, the cyber actors, as part of their October 2016 spear-phishing attack, resorted to creating a fake account to use in that spear-phishing campaign.

What did the cyber actors hope to achieve? What weakness was the spear-phishing 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.

What was the potential impact of the October 2016 phishing emails? Was this information later shared with customers?

Our understanding is that cyber actors sent an email from a fake account impersonating VR Systems and other elections companies. Because the email did not come from VR Systems and was not sent to VR Systems, we do not know who sent the email or who they sent it to. It is our understanding that all jurisdictions, including VR Systems customers, were notified by law enforcement agencies if they were a target of this spear-phishing attack.

After a thorough review, we have not been told by any of our customers that they clicked on the attachment or that any malware was downloaded. We have spoken to our customers and have no indication that any of their systems were breached. We are in regular contact with our customers and have shared everything we know with them. The impact of clicking on the attachment is unknown to VR Systems. We also provide advice to our customers on steps they should take to protect their systems from this and any other spear-phishing attacks.

What else is known about the October 2016 spear-phishing emails?

According to a leaked NSA report cited by media outlets, the cyber actors targeted 122 election officials. We do not know who the 122 officials are, and that information has not been officially provided to the public or VR Systems. We are led to believe among those 122 election officials, one or more may be our customers, but we do not have any evidence to support that.

What red flags were raised in the October 2016 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 election officials take to protect their 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 anytime and any hour, every day of the year and can respond immediately to a concern.

5) Secure all login 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 concerns should people have about security vulnerabilities going into the 2018 midterm election?

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 with our customers and is working in concert with security and law enforcement agencies to maintain robust and current security systems.

###