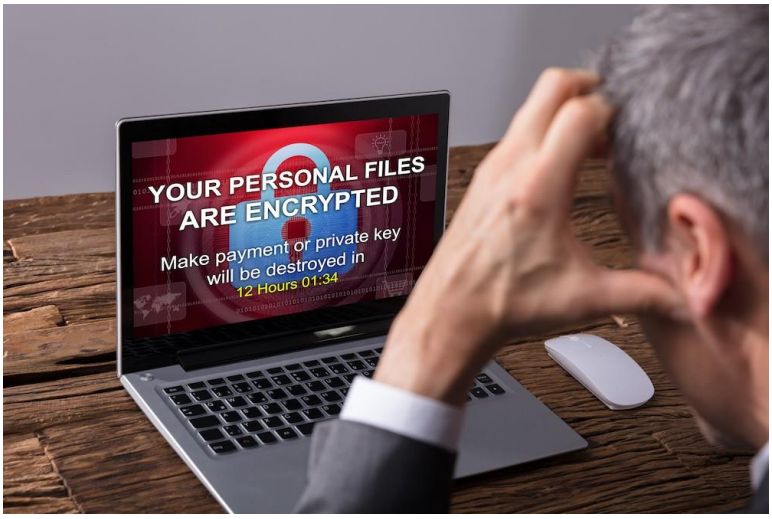
Ransomware victim shows why transparency in attacks matters



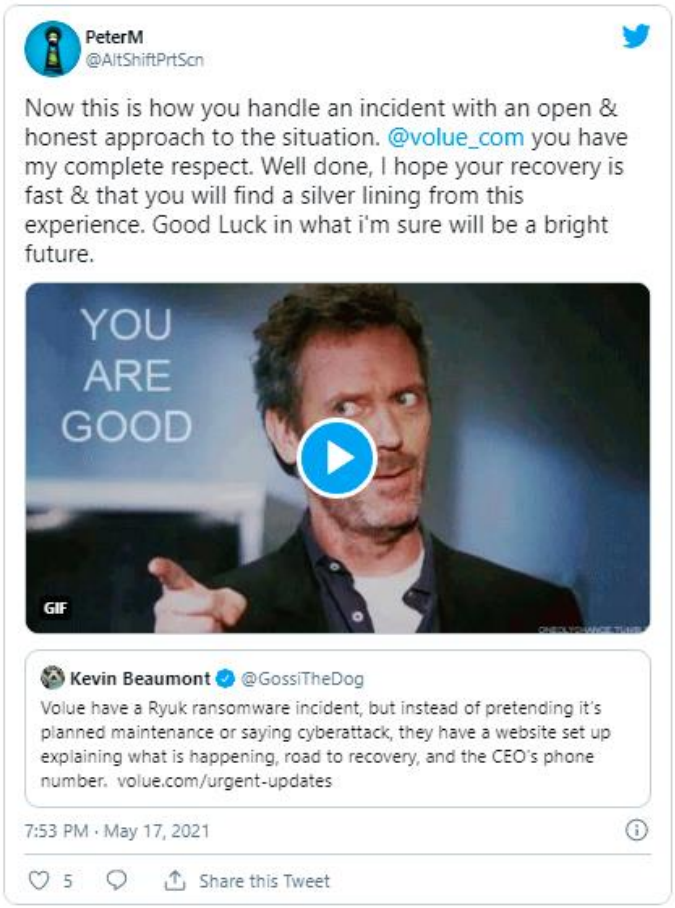
As ransomware attacks continue to wreak havoc in deep into employee workstations, companies still try to hide the attacks instead of being transparent. Thankfully, a group of researchers have discovered this one company and their unique way responding to an attack. We think that their ransomware attack recovery approach should be used as a model for all future disclosures.

On May 5th, green energy tech provider Volue suffered a Ryuk ransomware attack that impacted some of their front-end customer platforms.

Since then, Volue has been transparent about the cyberattack by providing webcasts, daily updates, and the email addresses and phone numbers for their CEO and CFO for questions about the attack.

In addition, the company states they have shared all indicators of compromise with KraftCert, a Norwegian Computer Emergency Response Team, to alert other companies and law enforcement. Volue's transparency is the exact opposite to the disclosures typically seen in ransomware attacks and should be used as a model for future disclosures.

This transparency has not gone unnoticed by cybersecurity professionals who are commending Volue's response to the attack.



Transparency looks a whole lot better, not worse

Transparency protects your customers and employees, inspires confidence in your company, and aids law enforcement, yet few companies choose to be transparent.

Instead, almost every ransomware victim first tries to hide an attack out of fear that it could cause reputational or legal harm.

Ultimately, the true nature of the attack is revealed after a malware sample or note is found, or the ransomware gangs publish data stolen during the attack.

Being transparent also allows breached companies to assist law enforcement in their investigations and prevent further attacks.

Finally, transparency inspires confidence with your employees, customers, and investors that the company is responding correctly to the attack and that there is nothing to worry about.

Recommendation

The FBI has urged victims to report ransomware attacks so they can receive fresh IOCs (indicators of compromise) about a ransomware operation.

When an organization is attacked, it is vital for law enforcement to quickly receive known IP addresses, files, and domains used by the attackers to be immediately analyzed and used as part of their investigations.

The longer a business waits to provide law enforcement with IOCs, the less useful they become as the attackers hide their traces or remote sites are shut down.

References

https://www.digitaluppercut.com/2020/12/what-does-ransomware-cost/

https://www.bleepingcomputer.com/news/security/ransomware-victim-shows-why-transparency-in-attacks-matters/?&web_view=true

https://www.govinfosecurity.com/2-bills-introduced-in-wake-colonial-pipeline-attack-a-16666?&web_view=true