CASE STUDY

Small Business Survives an Active Ransomware Attack

Malware continues to be a challenge for organizations of all sizes around the world. Unfortunately, the trend from the past few years is that malware and ransomware attacks are on the increase. Here are some sobering statistics:

A new organization fell victim to ransomware every 14 seconds in 2019 and is estimated it will be every 11 seconds in 2021. (CyberSecurity Ventures)

Phishing emails are the vector for two-thirds of ransomware infections. (Statista)

46% of ransomware operators impersonate authority figures such as the FBI or the IRS. (Stanford University)

eCrime, defined as criminal activities in order to generate revenue, have increased to 79% of all intrusions between 2019 and 2020. (CrowdStrike 2021 Global Threat Report)

As a Managed Service Provider (MSP), CoNetrix Technology has helped many customers secure their IT infrastructure against malware, and occasionally responded to malware attacks to stop or limit the damage. The purpose of this case study is to describe a specific malware attack against one of our customers and how the attack was successfully blocked. The goal is to provide information to other organizations so they can learn from this specific attack and better protect their IT environment.

DISCLAIMER

Every IT environment is slightly different, so strategies described in this case study may not apply to your situation.

Similarly, every attack is different, and the attack vectors are constantly changing. So over time the responses we describe in this case study may not apply for future attacks.

We are not disclosing any customer-specific information to protect their confidentiality and prevent making them a target for future attacks.

BACKGROUND AND CONTEXT: CUSTOMER'S IT ENVIRONMENT

Windows 10 virtual desktops available through Citrix Cloud and a hosted Citrix Remote Access Gateway.

Windows servers running on VMware vSphere.

Endpoint protection provided through CoNetrix Technology, based on CylanceProtect and CylanceOptics.

Email hosted with a different service provider using basic email filtering.

FortiGate Unified Threat Management appliance installed on the customer premise and managed by CoNetrix.

Identifying the Attack

At the beginning of this malware attack, our first Indicator of Compromise (IOC) was multiple alerts through the Cylance monitoring portal of attempts to install executables named like “remote.exe.” These were targeted at the virtual desktops hosted through Citrix.

Thankfully the attempts were blocked by Cylance, but the attackers continued with different executables trying to gain a foothold. Our research on these quarantined executables through tools like VirusTotal did not match any previously known malware.

INITIAL RESPONSE

- Increase Cylance Logging
- Add Egress Filtering
- Review Logs on the Fortigate and Citrix Gateway
- Change Passwords Immediately

Stopping the Attack

Our initial response was to locate the source of the attack by increasing logging through Cylance, implement egress filtering on the Fortigate, and review logs on the Fortigate and the Citrix gateway. We also requested the customer have their employees change their password immediately.

During our investigation, the attackers changed their tactics...

During our investigation, the attackers changed their tactics by moving to PowerShell based compromises and moving laterally by targeting different virtual desktops and different user accounts. As before, these attacks were **blocked by Cylance**. These changes in the attack vector provided some key information:

- This was not a simple automated attack. The bad actors were ***actively changing their approach*** in order to get a successful compromise.
- Multiple user passwords were likely hacked because the bad actors were attempting multiple accounts and we were not seeing failed logins in the domain security logs.

This activity continued over the next two days, and we were able to completely stop the attack by forcing all users to change their domain password and blocking IP subnets to the Citrix remote access gateway, which effectively cut off the bad actor’s access to the virtual desktops. During the attack, no systems were compromised and all malware was stopped by Cylance.

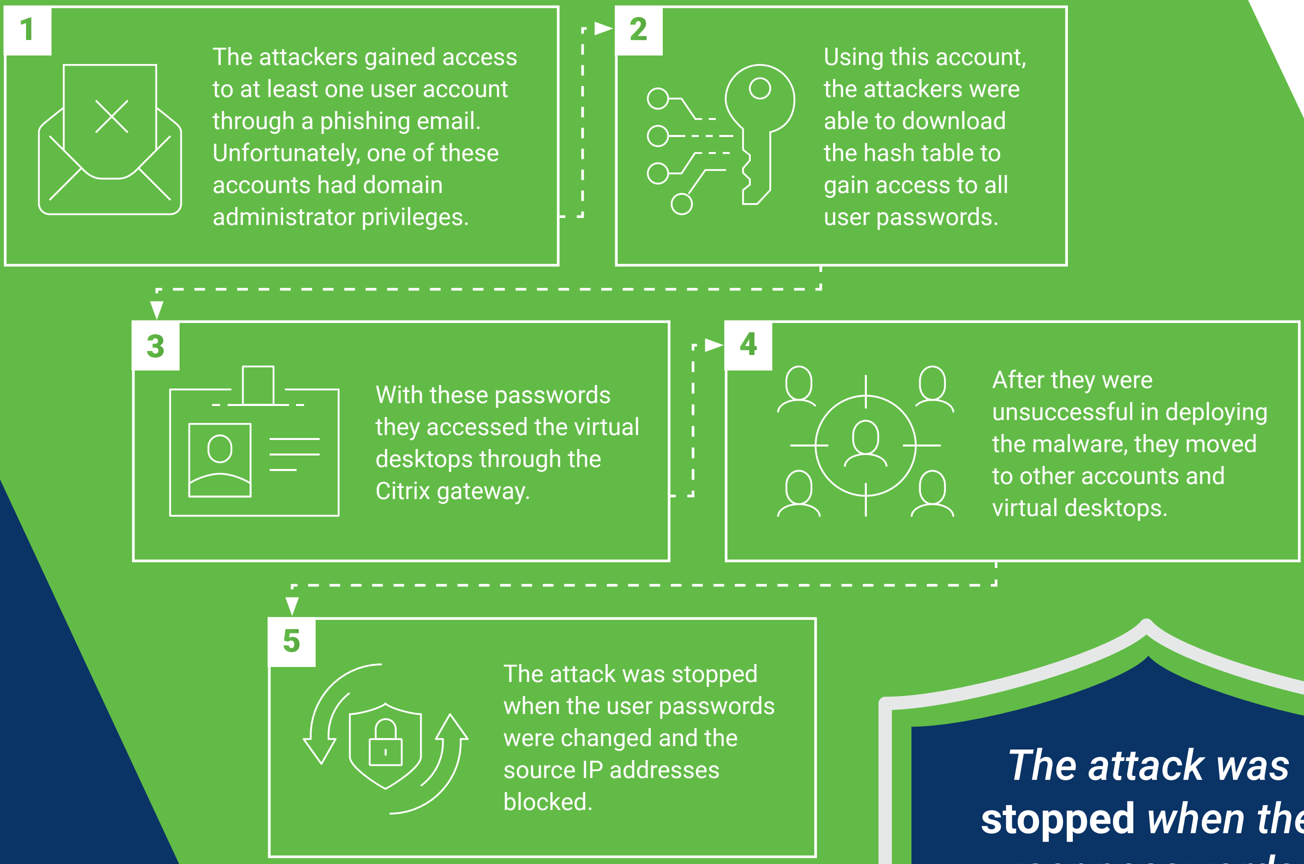
FINAL RESPONSE

- Force all users to Change their Domain Password
- Block IP subnets to remote access

During the attack, no systems were compromised and all malware was stopped by Cylance.

Analysis of the Attack

After completing our research into this incident we believe the attack began and progressed as follows:



1 The attackers gained access to at least one user account through a phishing email. Unfortunately, one of these accounts had domain administrator privileges.

2 Using this account, the attackers were able to download the hash table to gain access to all user passwords.

3 With these passwords they accessed the virtual desktops through the Citrix gateway.

4 After they were unsuccessful in deploying the malware, they moved to other accounts and virtual desktops.

5 The attack was stopped when the user passwords were changed and the source IP addresses blocked.

The attack was ***stopped*** *when the user passwords were changed and the source IP addresses blocked.*

Recommendations for Improvements to Prevent Future Attacks

While Cylance was effective in this situation and no malware was allowed to run, we recommended several improvements to the customer:

- ✓ Conduct security awareness training for all employees to help them identify phishing emails and avoid clicking on links in emails.
- ✓ Implement multi-factor authentication for remote access through the Citrix gateway. This would make it much more difficult to access a virtual desktop remotely if an account is compromised.
- ✓ Upgrade their email filtering solution with URL protection and active sandboxing of downloaded attachments.
- ✓ Limit the number of users with domain admin access, and not allow use of a domain admin account for regular “everyday” access.
- ✓ Strengthen policies for password length and complexity to make passwords less susceptible to cracking.

Key Takeaways

There are some additional key takeaways from this attack that apply to every IT environment:

- ✓ The best IT security consists of multiple layers and does not rely on a single technology. As an example, while Cylance worked in this situation, it would be risky to assume that any endpoint protection solution would be 100% effective in every attack.
- ✓ An Incident Response (IR) procedure should be defined in advance so you can respond quickly and efficiently to security incidents. This includes procedures for working with your IT vendor and your employees.
- ✓ Signature-based endpoint protection solutions are largely ineffective. This attack demonstrated that malware can be easily modified to circumvent any known signatures. An effective endpoint protection solution must use machine learning and behavioral analysis to stop current attacks. Cylance, CrowdStrike, and SentinelOne are the market leaders for this type of solution.
- ✓ Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) should be required for any external access to the network and access to any public cloud services, such as Microsoft 365. Despite our best efforts, end-users are not reliable for creating strong, secure passwords. MFA solutions such as Duo Security, RSA, and Google Authenticator can be effective defenses against a compromised password.

If you are interested in implementing any of these services, please contact us. A representative of CoNetrix Technology can match a solution to your specific situation.

BEST PRACTICES

- Add Multiple Security Layers
- Create an Incident Response Plan
- Implement Endpoint Protection with Machine Learning
- Require Multi-Factor Authentication

Malware attacks are constantly evolving, and IT administrators must adapt in order to protect their business. Hopefully, this case study demonstrates the value of a layered approach to IT security in order to provide the best protection.

About CoNetrix Technology

CoNetrix Technology is a computer networking, IT managed services, and private cloud hosting firm serving small businesses and financial institutions since 1977. Security is designed into all of our offerings. CoNetrix engineers hold numerous certifications from leading technology vendors, such as Microsoft, Cisco, VMware, Citrix, and others. Services include: Managed Security, Managed Network Support, Tier 1 IT Support, Network Design and Implementation, Disaster Recovery Planning, Voice Over IP, CyberThreat Assessment, and Private Cloud Hosting.

©CoNetrix, LLC. and CoNetrix Technology, LLC. All Rights Reserved. Partner names used with permission.

Don’t be a victim
of ransomware.

Reduce your risk and
fortify your cyber defense.

Ask us how we can help.

CoNetrix Technology

conetrix.com/technology | 800-356-6568 | techsales@conetrix.com