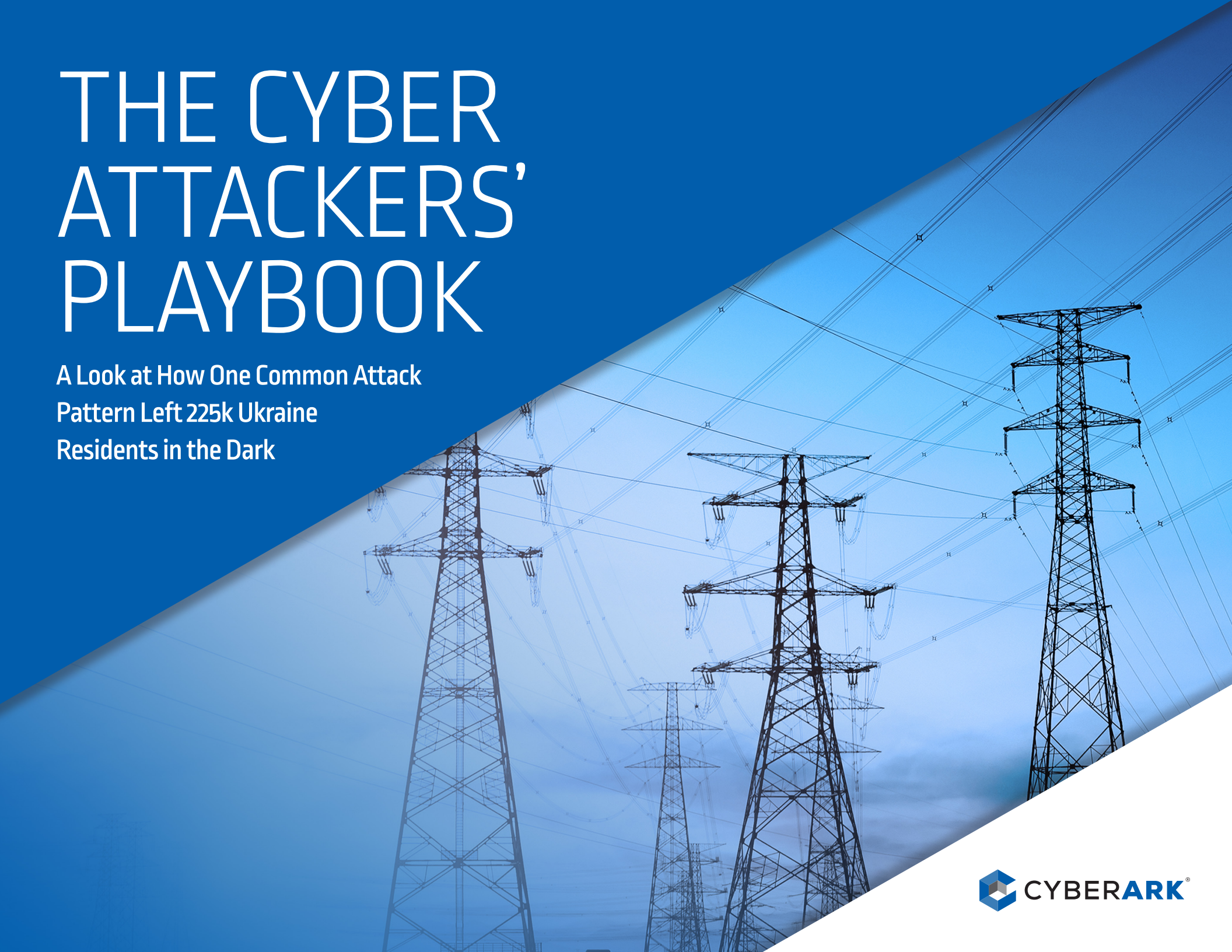
THE CYBER ATTACKERS' PLAYBOOK

A Look at How One Common Attack Pattern Left 225k Ukraine Residents in the Dark



CYBERARK®

Table of Contents

CHAPTER 1

INTRODUCTION

The Common Attack Pattern That Shut Down Power for Thousands of Ukrainians

INTRODUCTION

The Common Attack Pattern That Shut Down Power for Thousands of Ukrainians

On December 23, 2015, the western region of the Ukraine went dark. Two of the three local electricity providers were victims of a cyber attack—and an estimated 225,000 consumers were affected by its outcome. To make matters worse, the hackers took steps to impede swift remediation. With their IT and OT systems completely overwritten, power companies were left to manually fix the damage at individual substations throughout the region.

This event marked the first time in history that a cyber attack had successfully taken down a power system and disrupted the lives of everyday citizens. It provides a frightening example of just how much damage can be done when attackers gain access to an organization's network—and it follows a commonly used pattern that likely could have been broken, had utility companies taken the right preventative measures.

225,000
consumers were affected by the cyber attack on December 23

In this ebook, we'll examine this attack in more detail and identify common steps that are used time and again during advanced attacks. In the pages ahead, you'll discover:

- How phishing emails enabled attackers to break through the network perimeter
- How attackers stole credentials from compromised machines and used them to move laterally through the IT and OT environments
- How malware was used, not only as an attack tool but also to cause significant, costly damage to the utility companies' systems
- Proactive steps that you can take to stop attackers early in the attack cycle and prevent them from achieving their ultimate goals

CHAPTER 2

PHISHING

How an Email Gave Attackers the Access Needed to Turn off the Lights

CHAPTER 2: PHISHING

How an Email Gave Attackers the Access Needed to Turn off the Lights

In the attack against the Ukraine electric companies, spear phishing emails were used to target IT staff and system administrators. At least two individuals fell victim, opening malicious attachments that appeared to be from legitimate senders.

Once the emails and their attached files were opened, a malicious macro launched in the background and installed malware on the victims' machines. This malware provided the attackers with inside—yet limited—access to the power companies' networks. From there, the attackers were able to steal credentials from the local, compromised machines and use them to begin moving to connected systems.

Perimeter Compromise Steps

1. Spear phishing email opened by victim
2. Endpoints infected by malicious file
3. Attackers gain access through malware
4. Information and credentials are stolen

What you need to know about phishing scheme attackers and victims

Attackers are smart and motivated to succeed. As a result, they do their homework. Before casting a spear phishing line, they'll take steps to learn about the companies and users they are targeting.

How organizations can limit attackers' success:

- Educate users and encourage them to be suspicious of unexpected emails that contain attachments and links
- Keep systems patched to eliminate known vulnerabilities that can easily be exploited
- Control applications on endpoints to minimize an attacker's ability to successfully infect victims' machines with malware
- Remove local admin rights from standard users to limit what an attacker is able to do in the event of a system compromise

There is a 90+% chance that at least one person will fall prey to attackers when a mere 10 emails are used in a phishing campaign.[1]

CHAPTER 3

CREDENTIAL THEFT

How Attackers Used a Single Foothold to Compromise the IT and OT Environments

CHAPTER 3: CREDENTIAL THEFT

How Attackers Used a Single Foothold to Compromise the IT and OT Environments

Once the attackers had an initial foothold inside the Ukrainian utilities' network, they were able to steal and guess passwords until they ultimately gained access to an administrative account within the IT network. With this limited administrative access, they were able to escalate privileges, compromise most of the IT systems, and gain access to additional privileged accounts—including one that provided VPN access into the OT network. Through the VPN, they gained full access to the Human Machine Interface (HMI) systems in the control room, and thus access to the grid systems.

For several weeks, the attackers operated covertly. As they compromised more and more IT systems, they also installed dormant but highly destructive KillDisk malware that could be remotely activated at a later time. Inside the control room, they simply watched and learned. They identified how operators accessed and controlled systems, and how firmware updates were remotely applied to substations in the field. Only later, once they were ready, would the attackers put their knowledge and compromised privileged access to use to execute the final stages of the attack.

Lateral Movement and Escalation Steps

1

Attackers steal and guess local administrator passwords

2

Compromised passwords are reused to access more systems on the domain

3

By elevating privileges, attackers gain control of IT systems across the network

4

Privileged VPN credentials are compromised to allow crossover into the OT network

How to mitigate credential theft risks and limit an attacker's ability to move through IT and OT systems

- Use multi-factor authentication in as many places as possible
- Frequently change administrative passwords to limit their usable life
- Require local administrator passwords to be unique on each system, to limit lateral movement
- Proactively secure and monitor the use of high-value accounts, such as domain accounts and accounts that can control critical infrastructure
- Analyze privileged user and account behavior to detect anomalous activity that may indicate credential theft or the presence of backdoor accounts
- Segment sensitive areas of the networks and isolate privileged access to critical systems to reduce the attack surface

An estimated

80-100%

of the most serious cyber attacks involve the misuse or abuse of privileged credentials, according to incident responders.[2]

CHAPTER 4

ACHIEVING THE END GOAL

How Attackers Caused a Massive Blackout and Destroyed Systems to Prevent Swift Remediation

CHAPTER 4: ACHIEVING THE END GOAL

How Attackers Caused a Massive Blackout and Destroyed Systems to Prevent Swift Remediation

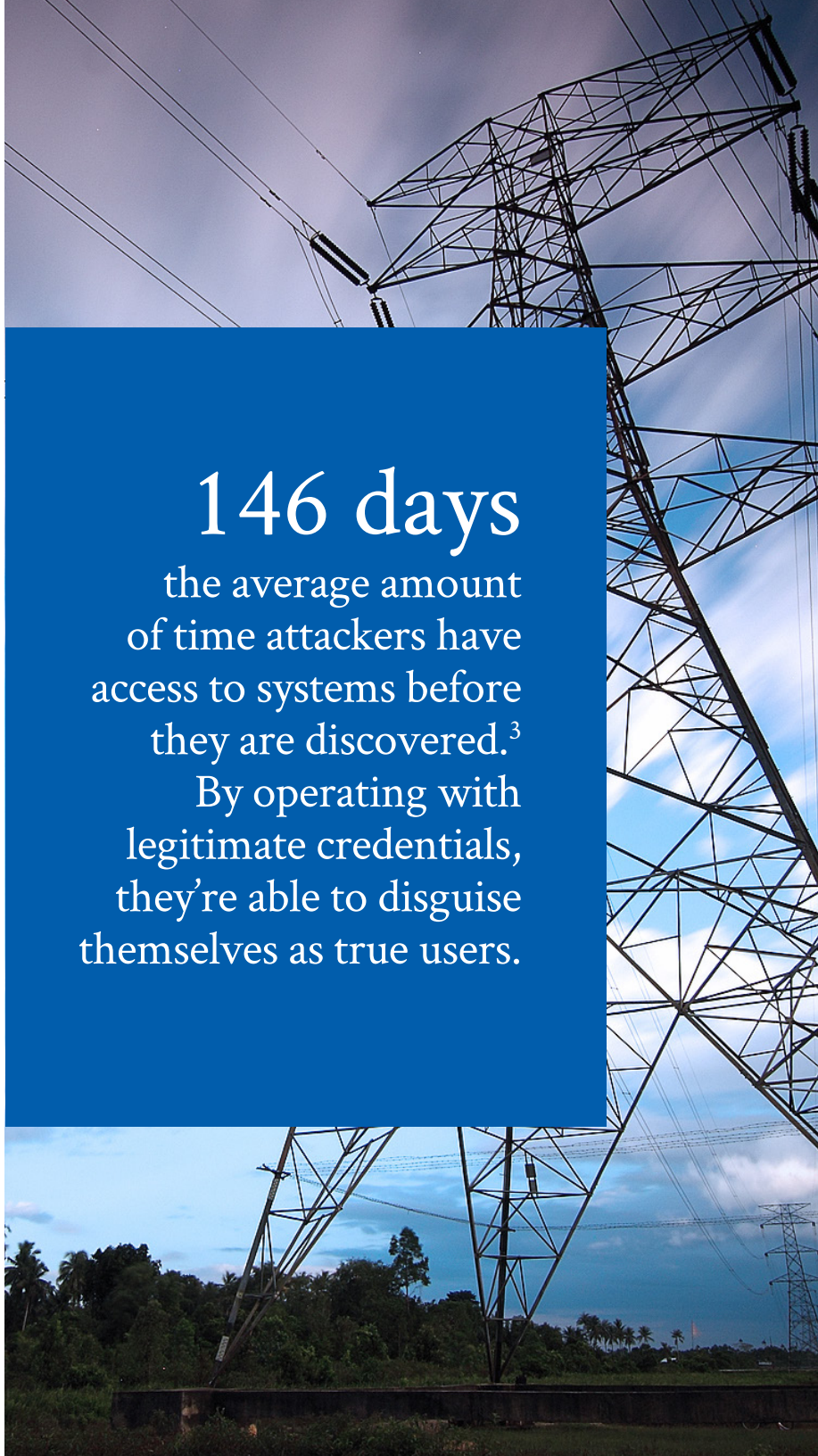
Much like other, similarly patterned attacks, the Ukraine incident involved hackers being inside company networks for months before they actually executed their ultimate plan. All that time, they were learning the network and systems— while operating under the guise of authorized users— and making preparations for December 23rd.

By the time the lights went out, the attackers had opened breakers and shut down electricity at 30 substations, issued a firmware update to 16 substations to make them completely unresponsive to remote commands, and disabled backup power supplies. To prevent swift remediation, they activated the previously dormant KillDisk malware that overwrote IT systems and wiped master boot records. Lastly, they launched a DDoS attack, overwhelming the utility companies' call centers so that customers couldn't report outages.

To finally get electricity back up and running, utility workers had to drive to power stations and manually reset breakers. Even three months after the attack, breakers were still being manually controlled.

What enterprises can do to better detect malicious users and minimize their damage

- Control and monitor applications to help prevent malware
- Secure and frequently change privileged credentials to limit an attacker's ability to compromise and use privileged accounts
- Analyze user and account behavior to identify anomalous activity that could indicate compromised credentials
- Segment the network to limit access to sensitive IT systems
- Isolate access to critical systems to reduce their attack surface, and closely monitor all traffic to those systems
- Examine user activity during privileged sessions to quickly detect advanced and inside threats



146 days

the average amount of time attackers have access to systems before they are discovered.[3] By operating with legitimate credentials, they're able to disguise themselves as true users.

CHAPTER 5

CONCLUSION

The Role of Privileged Accounts and 12 Practices That Could Have Helped Prevent the Attack Outcome

CHAPTER 5: CONCLUSION

The Role of Privileged Accounts and 12 Practices That Could Have Helped Prevent the Attack Outcome

Privilege plays a key role in the type of attack that was seen in the Ukraine. In the case of that unprecedented incident, privilege was exploited when:

- Administrative credentials were captured from infected endpoints
- The compromised credentials allowed hackers to move through the IT environment and escalate privileges
- Compromised VPN credentials were used to breach the OT environment Attackers used comprised privileged accounts to shut down power grids, corrupt OT systems, and wipe endpoints and servers

12 best practices that can help break the attack pattern

Because the activities seen in the Ukraine represent such a common attack cycle, there are a variety of steps enterprises of all types can take to prevent them. These include:

Endpoint protection

1. Encourage users to be suspicious of unexpected emails
2. Patch systems to remediate known vulnerabilities
3. Control applications to minimize malware infection risks

4. Remove local admin rights from standard users

Credential security and control

5. Use multi-factor authentication widely
6. Change administrative passwords frequently
7. Require unique local administrator passwords on each system
8. Proactively secure and monitor the use of high-value accounts
9. Segment the network to limit access to sensitive IT systems
10. Isolate and restrict access to critical systems

Privileged threat detection

11. Analyze user and account behavior to detect anomalous activity
12. Examine privileged session activity to detect insider threats

Ready to take the next step toward securing your privileged accounts and protecting your organization from attacks?

Visit cyberark.com to request a free risk assessment, today.

Sources for Ukraine attack story:
http://www.eweek.com/security/attacks-on-ukrainian-power-providers-hold-lessons-for-the-future.html

http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[1] Verizon, "2015 Data Breach Investigations Report"

[2] CyberArk Threat Report, "Privileged Account Exploits Shift the Front Lines of Cyber Security"
https://www.cyberark.com/threat-report/

[3] Mandiant MTrends, 2015

CYBERARK®