MICROSOFT DETECTION AND RESPONSE TEAM
INCIDENT RESPONSE CASE REPORT // 002

FULL OPERATIONAL SHUTDOWN

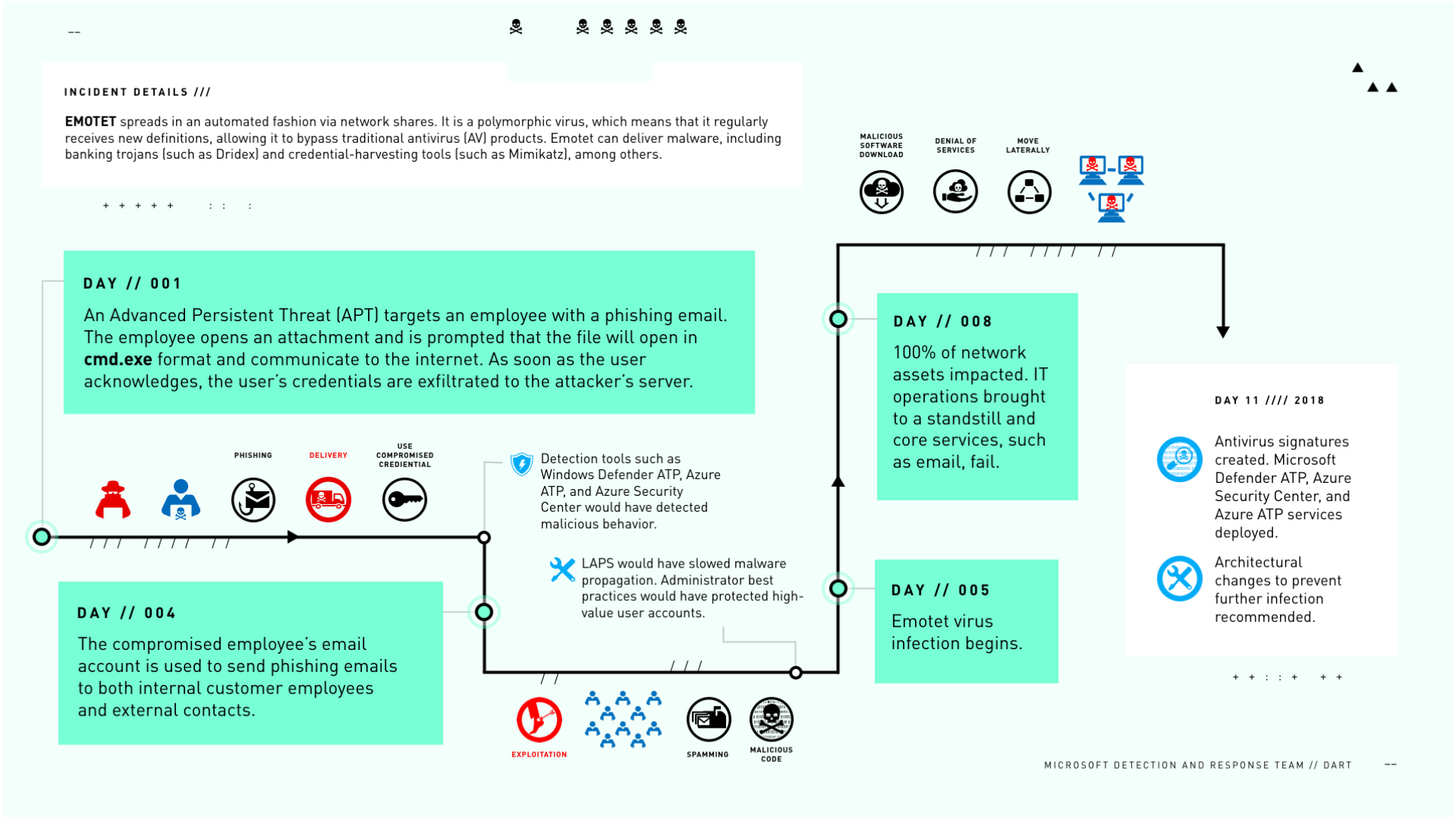
002

THE STORY OF HOW A POLYMORPHIC VIRUS SHUT DOWN AN ORGANIZATION'S ESSENTIAL SERVICES, AND HOW DART CAME TO THE RESCUE

Incident Response Case Report 002 is part of the report series focusing on stories from the cybersecurity frontlines by the Microsoft Detection and Response Team (DART).

After a phishing email delivered Emotet, a polymorphic virus that propagates via network shares and legacy protocols, to Fabrikam,[1] the virus shut down its core services. It dodged antivirus detection through regular definition updates from an attacker-controlled command-and-control (C2) infrastructure, and spread through the company's systems, causing network outages and shutting down essential services for nearly a week.

[1] *Fabrikam is a pseudonym to protect the confidentiality of an actual DART customer.*



HOW DID IT BEGIN?

When the last of their machines overheated, Fabrikam knew the problem had officially spun out of control. "We want to stop this hemorrhaging," an official would later say. He'd been told the organization had an extensive system to prevent cyberattacks, but this new virus evaded all their firewalls and antivirus software. Now, as they watched their computers blue-screen one by one, they didn't have any idea what to do next.

Here's what we know for sure. A threat actor sent a swarm of

phishing emails to Fabrikam employees. Even with Verizon reporting that the click rates of phishing emails is down to three percent, one Fabrikam employee opened a file attached to a phishing email and a cmd.exe whisked their credentials away to the phisher's server. At that point, the phisher controlled the employee's machine.

What the employee didn't know was that allowing that attached executable to communicate to the internet was all part of a threat actor's plan to spread Emotet throughout Fabrikam's network. Emotet is a highly automated, commodity malware used to gather vital information on organizations and the people who work in them. Using banking trojans and credential-theft tools, it collects data to steal money, commit fraud, and impersonate individuals. The threat actor may use this information themselves, or they may sell the information on the dark web to other attackers hungry for a fresh opportunity.

Four days after gaining a foothold, the threat actor used their control over the employee's computer to start sending out phishing emails to other people within the Fabrikam network. This is an insidious and effective way to infect a network. Many common email filters don't scan internal messages for malware, and phishing emails from an internal account look even more convincing to the naked eye. More people clicked attachments; more machines downloaded malware. Everything was going according to the threat actor's plan.

One of the worst things about Emotet is how slippery it can be to detect. It's a polymorphic virus, which means it updates itself with new definitions every few days. This is how it stays one step ahead of antivirus software. Working via admin accounts, it spread credential-stealing trojans across employee accounts and used them to authenticate itself within the network. Fabrikam didn't have any network visibility tools in place, so for the next twenty-four hours Emotet wormed its way through its infrastructure without raising any red flags. Then, the threat actor brought the whole network down.

DART deployed trial licenses of Defender Advanced Threat Protection, Azure Security Scan, Azure Advanced Threat Protection services, and other Microsoft special-purpose malware-detection tools.

WHAT WAS THE EFFECT?

That Saturday, most of the Fabrikam offices had closed for the weekend, so no one may have even noticed the first machines freezing as their CPUs maxed out. Then the effect dominoed out across Fabrikam and its critical systems, which began to fail. Officials announced that the virus threatened all of Fabrikam's systems, even its 185-surveillance camera network. Its finance department couldn't complete any external banking transactions, and partner organizations couldn't access any databases controlled by Fabrikam. It was chaos.

The cybersecurity term for this event is "distributed denial of service" (DDoS)—when a threat actor uses multiple compromised computers to flood a network with internet traffic until it's overwhelmed. The effects can be devastating. In a 2017 survey, Kaspersky Lab reported that the average cost of an enterprise-level DDoS attack was $2 million. Nearly a quarter of victims also reported a loss of revenue, business opportunities, and reputation among clients and partners. If this is true, Fabrikam should consider itself lucky—its reported damages would total a little over $1 million.

The virus threatened all of Fabrikam's systems, even its 185-surveillance camera network. Its finance department couldn't complete any external banking transactions, and partner organizations couldn't access any databases controlled by Fabrikam. It was chaos.

Back at the headquarters, the IT department scrambled. They had a good team, but they'd never dealt with this kind of attack before. They couldn't tell whether an external cyberattack from a hacker caused the shutdown or if they were dealing with an internal virus. It would have helped if they could have even accessed their network accounts. Emotet consumed the network's bandwidth until using it for anything became practically impossible. Even emails couldn't wriggle through. Their phones rang off the hook. The boss kept calling for status reports. They needed help. They needed someone who's faced these problems before, a triage team with access to world-class threat intelligence, experts in Windows infrastructure, and forensics specialists who could pull apart network logs, identify the original attack vector, and tell them how the threat actor moved laterally through the network.

That afternoon they called us.

HOW WAS IT RESOLVED?

Eight days after the initial phishing email, Fabrikam procured Microsoft Premiere Support, connecting them with our Cybersecurity Solutions Group's Detection and Response Team (DART).

Our DART organization is a global collection of cybersecurity incident-response specialists, highly skilled in detecting the most current attacks and assisting customers during security crises, particularly when they occur on Windows-based systems. DART utilizes its expertise, as well as custom tools, including specialized detection tools, malware analysis, signature generation, and custom cyberintelligence, for signs of advanced implants not typically found by commodity antivirus or intrusion-detection system technologies, which was exactly the type of problem Fabrikam faced.

While one group of DART specialists went onsite with Fabrikam, other members began to help remotely. With the systems Fabrikam had in place, DART had no visibility or control over the threat actors' operations, so DART deployed trial licenses of Defender Advanced Threat Protection, Azure Security Scan, Azure Advanced Threat Protection services, and other Microsoft special-purpose malware-detection tools. With a lens into the environment, DART's forensics experts and reverse engineers started combing Fabrikam's logs to uncover what happened.

The organization had never experienced an attack like this before, and they hadn't set up the security best practices to address the problems they were facing. "Shame on us," the IT director told Fabrikam's board, "for doing a disservice to our intelligence community."

When DART's onsite team arrived, they found the Fabrikam IT team exhausted. Core services had been down for days. The previous week they had worked like a bucket brigade, trying keep things afloat. C-levels had called emergency meetings to evaluate the incident and gave press conferences to soothe the public's concerns. The organization had never experienced an attack like this before, and they hadn't set up the security best practices to address the problems they were facing. "Shame on us," the IT director told Fabrikam's board, "for doing a disservice to our intelligence community."

Our team sat down with theirs and whiteboarded everything about the attack: the DDoS, the phishing emails, the virus. Then, they came up with a plan. They needed to make architectural changes in the network to stop the spread of Emotet, and then to put administrative best practices in place to contain and eradicate the virus.

Using the tools set up remotely, the onsite DART specislists got into the network and implemented asset controls, creating buffer zones separating the assets with administrative privileges in the environment. For the first time in a week, Emotet wasn't pinballing between Fabrikam's machines and reinfecting machines that had been cleaned. These buffer zones contained the virus enough to remove it with antivirus software. With the architecture in place and detection tools deployed, DART uploaded antivirus signatures and eradicated the Emotet virus. Onsite reverse engineers then began repairing the Microsoft System Center Configuration Manager, and soon Fabrikam was back on its feet.

Then, they came up with a plan. They needed to make architectural changes in the network to stop the spread of Emotet, and then to put administrative best practices in place to contain and eradicate the virus.

Microsoft DART is comprised of senior IT leaders and security experts with extensive experience in both the private sector and government. Many are former military, intelligence, and law enforcement members with deep cybersecurity backgrounds. DART engagements are delivered by these experienced cybersecurity professionals who devote 100 percent of their time to providing reactive and proactive cybersecurity services to customers worldwide.

WHAT CAN WE LEARN?

Part of the problem that Fabrikam faced were failures in best practices. Their email filters didn't cover internal emails, meaning the threat actor spread the virus without alerting anyone. If network visibility mechanisms had been in place, the early malicious behavior could also have been detected. The virus's spread could have been slowed and high-value accounts could have been protected if Fabrikam's administrative directories had not been wide open to exploration.

The other issue Fabrikam faced was that their IT team didn't have experience with these sorts of attacks. While they were skilled at dealing with the issues they faced day-to-day, advanced persistent threats vary widely in tactic,s and implementing an emergency response plan can be much more difficult than it appears on paper. They needed access to individuals who could cover the skill gaps in their own IT team and had emergency response experience.

What can be done then to minimize exposure to similar attacks?

01

Email filtering tools like Office 365 Advanced Threat Protection (ATP) would have detected and stopped the propagation of the malware.

02

Multi-factor authentication could have slowed or stopped the use of compromised credentials.

When traditional defenses fail, network visibility via advanced detection tools is critical. Detection tools such as Defender ATP, Azure Security Center, and Azure ATP would have identified malicious behavior and could have stopped it before it spread from the initially infected machine.

Microsoft's Local Administrator Password Solution provides management of local account passwords for domain-joined computers. It stores passwords in the active directory and protects it through access control lists, so only eligible users can read it or request its reset.

03

Configuration management, timely patching, and antivirus definition updates remain essential to defensive operations.

Best practices to protect and segment administrative privileges would have slowed the virus's propagation. Microsoft's Directory Tier Administrative Model reduces the impact of breaches caused by poor access control by protecting high-risk PCs and valuable assets like domain controllers.

Microsoft offers a varety of solutions as well as benchmarks for security configurations. DART currently offers a Security and Crisis Response Exercise for organizations to train their in-house teams on incident response scenarios. Microsoft has also partnered with the Center for Internet Security (CIS) to develop benchmarks to provide prescriptive guidance for establishing secure baseline configurations for Microsoft 365 and Azure.

Stay tuned for more DART Case Reports from the incident-response frontlines...

MICROSOFT DETECTION AND RESPONSE TEAM // DART

Microsoft