CASE STUDY

IDENTIFYING THE UNKNOWN

IDT gains full thread-level visibility into its endpoints with Secdo

BACKGROUND

Established in 1990, IDT Corporation (NYSE: IDT) is a multinational telecommunications company headquartered in Newark, NJ. The company has several subsidiaries, including IDT Financial, and has spawned various other successful companies such as Genie Energy (NYSE: GNE) and Straight Path Communications (NYSE: STRP), to name a few.

Today, IDT employs over 1,400 people globally and, through its IDT Telecom division, is the industry leader in telecommunications and payment services, as well as one of the world's largest providers of international voice termination. IDT is also one of the fastest growing international carriers, with revenues exceeding $1.6 billion.

CHALLENGES

IDT’s offering spans across multiple industries, requiring it to manage thousands of endpoints and servers across international borders, along with data that’s hosted in a hybrid cloud. This infrastructure in itself creates an extremely broad attack surface.

IDT has been the target of a daily dose of sophisticated cyber-attacks by state-sponsored actors, criminals, hacktivists, and even script kiddies—hackers of every stripe, motivation, and skill level. The company mitigates hundreds of attacks on a daily basis, according to its CIO, Golan Ben-Oni. “Each industry comes with its own attack surface, its own adversaries, and challenges. We are in a number of vertical markets which are each individually targeted. So the number of attacks that we see in comparison to other organizations is typically higher.”

Golan Ben-Oni, CIO

FOUNDED
1990

HEADQUARTERS
New Jersey, USA

EMPLOYEES
1,400

INDUSTRIES SERVED
Telecommunications, Energy and Oil, Banking and Finance, Media and Entertainment, Pharmaceutical, Education

OPERATIONS
20 countries

RESULT
Greatly improved endpoint visibility and threat hunting capabilities.

As if the above wasn't enough of a challenge, the attacks are becoming more sophisticated and invasive. Stopping cyber criminals from slipping inside enterprise networks and getting their hands on sensitive data is extremely challenging in the current thread landscape. "In cybersecurity, there is no silver bullet. No matter how many detection and prevention systems you deploy, an enterprise must be ready for what happens when it does get compromised," said Ben-Oni.

And Ben-Oni knows what he's talking about when he warns against sophisticated attacks that outsmart detection and prevention systems—on April 29th, 2017, two weeks before the WannaCry ransomware attack outbreak, IDT was hit with an attack that Ben-Oni, a veteran cybersecurity professional with over two decades of experience, had never seen before. *In this interview with The New York Times*, Ben-Oni warned, "the world is burning about WannaCry, but this is a nuclear bomb compared to WannaCry. It's a lot worse. It steals credentials...and it's happening right under our noses."

The attack against IDT leveraged NSA toolkits that were released publicly by hacker group The Shadow Brokers in 2016, and was an early warning for what took place internationally a month later with the Petya and NotPetya ransomware attacks. The attackers used identical tools, methods, and procedures. However, the attack went completely unnoticed by IDT's other detection and prevention tools. It wasn't even reported by any of the 128 publicly available threat intelligence feeds that IDT subscribes to, nor the 10 paid threat intelligence feeds the company spends nearly a half-million dollars on every year.

> *"The world is burning about WannaCry, but this is a nuclear bomb compared to WannaCry. It's a lot worse. It steals credentials. You can't catch it, and it's happening right under our noses."*

It was a very complex credential-theft attack for various reasons. First, it remained in memory as a single thread within a legitimate process, reprogramming it as it took it hostage—something only thread-level visibility into endpoint activity would be able to identify. It also attempted to move laterally throughout the organization, which could've easily done so and remain undetected all along. For years, the industry has emphasized the importance of keeping software current with the latest patches, but even systems that have been fully patched would've been vulnerable to this attack.

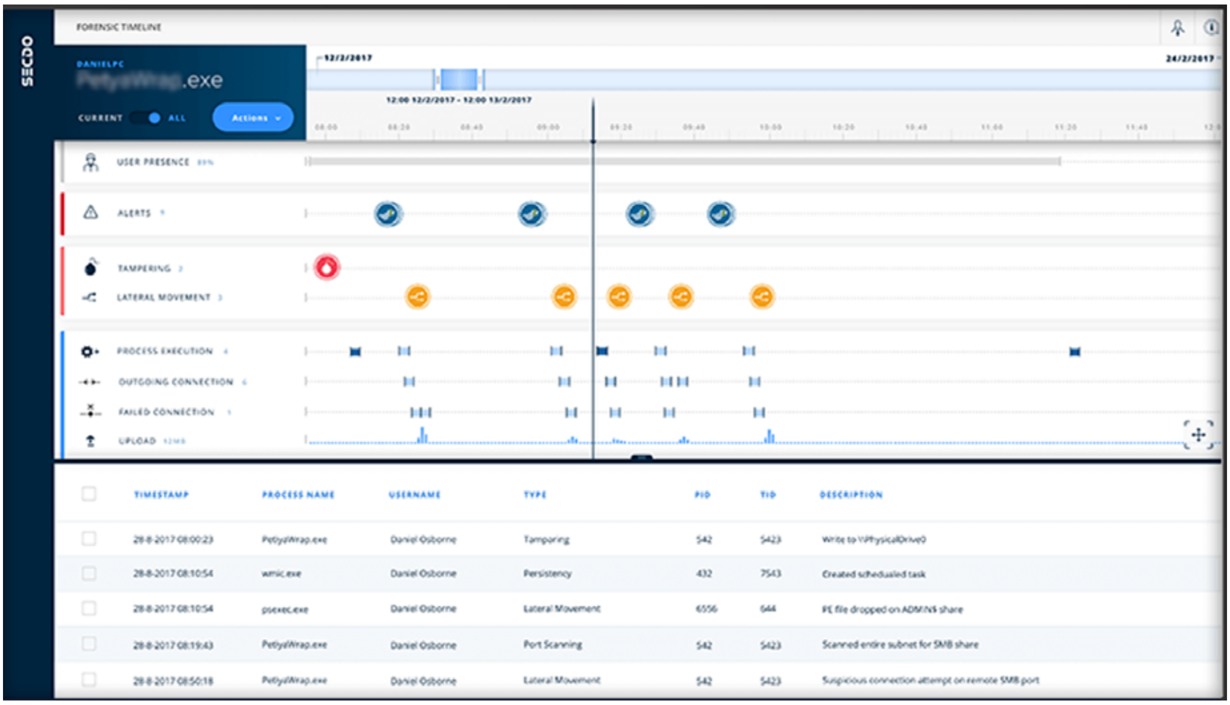
SOLUTION

IDT had deployed Secdo on all its endpoints and servers a year prior to the April attack. Secdo continuously records all endpoint activity at the thread level, the single most granular view possible into activity on endpoints. Data is stored on a centralized server—either on-premise or in the cloud—which allows IDT not only to maintain a backup of data that can be trusted if any endpoint were to be compromised, but to go back in time as far as needed if an investigation were to require it. Secdo automatically analyzes all endpoint data, enabling IDT's security team to proactively hunt for threats and investigate any lead or alert back to the attack chain and its root cause. From there they can assess the damage, affected hosts, and other behaviors. Once a real threat is found, Secdo provides a wide set of response and remediation tools that can be operated remotely and surgically, allowing IDT to maintain business productivity and continuity.

In the case of the April attack, Secdo had successfully recorded everything on IDT's enterprise and production networks. "Had Secdo not been running on our endpoints at the time of the incident, we wouldn't have known about it. We would've been left with a machine that was locked by ransomware and wouldn't have any knowledge about what happened," Ben-Oni adds.

The ability to get full visibility into endpoint activity at the thread-level—making it possible to identify behaviors that could've easily gone unnoticed by tools without the same depth of visibility—became extremely valuable during the April attack on IDT's systems. It helped IDT's security team identify the attack (that all other detection and prevention solutions missed), understand what damage was done, and contain it before it could spread into additional endpoints and cause more damage.

> *"Have we not had Secdo running we would not have come to the close visibility that we had to reconstruct the attack. We wouldn't have known about it."*



□	TIMESTAMP	PROCESS NAME	USERNAME	TYPE	PID	TID	DESCRIPTION
□	28-8-2017 08:00:23	PetyaWrap.exe	Daniel Osborne	Tampering	542	5423	Write to \\PhysicalDrive0
□	28-8-2017 08:10:54	wmic.exe	Daniel Osborne	Persistency	432	7543	Created schedualed task
□	28-8-2017 08:10:54	psexec.exe	Daniel Osborne	Lateral Movement	6556	644	PE file dropped on ADMIN$ share
□	28-8-2017 08:19:43	PetyaWrap.exe	Daniel Osborne	Port Scanning	542	5423	Scanned entire subnet for SMB share
□	28-8-2017 08:50:18	PetyaWrap.exe	Daniel Osborne	Lateral Movement	542	5423	Suspicious connection attempt on remote SMB port

RESULT

Faced with a constant barrage of cyber-attacks, IDT's security team utilizes Secdo's incident response and threat-hunting platform to gain visibility into the activity on each endpoint and server at the thread level, investigate any lead or alert, and respond to incidents surgically.

IDT continuously uses Secdo to:

Record all endpoints activity across the enterprise

Maintains a log of all activity—including files, processes, threads, network communications, users, registry, removable media, and more, at unparalleled depth—and provides the ability to go back in time (months or even years, depending on the user's preferred configuration) to thoroughly investigate incidents.

Investigate any incident

Allows IDT to determine the root cause of an incident, understand attack methods and patterns, assess damage, and identify possible remediation steps—all in only a few clicks.

Bridge the gap between the network and endpoint security

Streamlines incoming alerts by integrating with firewalls, antivirus, and any threat detection tool to automate response the moment something suspicious is flagged.

Contain infected hosts

Freezes targeted processes in memory and isolates endpoints as needed to prevent lateral movement of malware during mitigation and containment.

Respond to threats surgically

Eliminates impact on business productivity and continuity by allowing IDT to respond and remediate threats remotely, on one or multiple endpoints at a time. IDT analysts can choose to quarantine processes and suspicious files, isolate endpoints, freeze targeted processes, conduct live forensics, make changes to an endpoint via live access to the terminal, capture screen activity from an endpoint, retrieve or upload a file, etc.

Create alerts for exploits and behaviors

Lets IDT create BIOCs (behavior-based indicators of compromise) based on the attack's methods and patterns as revealed during the investigation, allowing the system to catch similar attacks in the future.

Minimize the risk of future attacks

Enables IDT's security team to identify gaps and blind spots in their defenses, and to address them ahead of future attacks.