

Special Report

GOVERNMENT
CYBERATTACKS:
**PROACTIVELY SECURE
YOUR INFRASTRUCTURE**



Government agencies and organizations have the added responsibility to protect the networks and data they use as a duty to the people they serve. These agencies are also more targeted than most corporations, as the data for which they are responsible is of great value to the attackers. This can be seen in the increase in government breaches over the past five years, as well as the sheer number of records that have leaked, from an average of less than 75 from 2014 to 2017, to over 100 breaches in 2018. As for the records obtained, this is where we see the biggest jump, with more than 9 million records in 2014 to nearly 82 million in 2018 (1).

Government breaches have risen over the years. The United States Senate's Federal Cybersecurity: America's Data at Risk report clearly states the following:

“The number of data breaches agencies have reported in recent years is not surprising given the current cybersecurity posture of the federal government. A recent report by the Office of Management and Budget made clear that agencies ‘do not understand and do not have the resources to combat the current threat environment.’”



The same report exposed that the past ten years of audits on eight of the top government departments failed to protect personal identifiable information (PII), relied on outdated systems/software, and failed to install security updates.

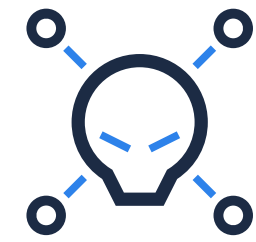
The Office of Personnel Management (OPM) is one of the greatest examples of security failures for the government. In 2015, two security breaches exposed 26 million current and former government employees' information, as well as 5.6 million stolen fingerprints. After such a gross display of security negligence, one would think that the agency would harden its security immediately. However, in 2017, the 19 recommendations made by the United States Computer Emergency Readiness

Team were not fulfilled. Only 11 were completed, and eight required further improvement.

It is essential to note that the OPM agency did not even have the correct monitoring solutions in place during these breaches. It was only after installing a few security solutions that the agency realized they had been breached. This gross negligence is commonplace in so many areas of the government where breaches occur without the IT staff even knowing there is an issue.

All of this goes back to the Senate's observation that agencies don't understand the environment they have, much less how to properly secure said environment.





TYPICAL BREACHES

Despite the narrative of hyper-complex attacks penetrating rock-solid defenses, subsequent investigations tend to show trivial attacks exploiting obvious security gaps. Under normal circumstances, forensics rapidly uncover the root issue that allowed the breach to occur. There are many reasons permitting a breach, which is one reason why eliminating breaches is so difficult. A short list of why breaches occur includes the following:

- Unpatched applications – applications are an easy target for an attacker due to the volume of computers on which the application is installed. If one security hole is found in an application, then every other installation of the application is vulnerable. Application vendors release patches, but it is up to the individual users or the IT staff to deploy this patch to fix the security issue in the application. History has shown that patching applications is nowhere near 100 percent, which gives the attacker an easy target.
- Unpatched operating systems – attackers have become proficient in finding security holes in operating systems. As with applications, a known vulnerability in an operating system is open to any attacker until the security hole is fixed. Even with the massive attention that has been given to Microsoft security patches, Patch Tuesday, and elevation of security patches, attackers constantly prove that unpatched systems are everywhere and easy to strike.
- Weak or incorrect security settings – there are security settings for applications, operating systems, user environments, browsers, network communications, and more. Often, vendors settle for weak security to prioritize communications and compatibility. This means that it is up to the IT staff to harden all the different areas of the computing environment.
- Security Drift – this a phenomenon that plagues every IT staff and their computing environment. Security drift is the reality that settings, privileges, controls, etc. over time become configured insecurely. This might be the Domain Admins group, a firewall setting, or a password policy control. Although Drift is usually much more common in larger organizations, smaller organizations are not exempt.

These are certainly not the full extent of the cornerstones for a breach, but they are present in more than a small percentage of breaches.





CASE IN POINT

In January 2020, reports emerged that the United Nations Active Directory network and associated data had been compromised. The breach is not being debated, but the details of the breach need to be addressed, understood, learned from, and acted upon to secure every Active Directory installation.

Both a leaked report and direct interviews seem to contradict the alleged severity of the breach and the current security situation of the network. It is important to unveil the details to see where there might be confusion around the context of the breach and exactly what occurred.

First, a UN spokesperson declared: “The damage related to this specific attack has been contained, and additional mitigation measures implemented.”

This detailed report unambiguously stated that: “Technicians at the United Nations office in Geneva, the world body’s European hub, on at least two occasions worked through weekends in recent months to isolate the local U.N. data center from the internet, re-write passwords and ensure the systems were clean. Twenty machines had to be rebuilt, the report says.”

⚠ Consider the breadth of the breach if a team must work through two weekends to fix the issue. If you’re reading this, you know exactly how long it takes to build a server, and if “twenty machines had to be rebuilt,” then these cannot be endpoints, but UN servers! The two-week time frame would seem reasonable.



The report continues: “The internal document from the U.N. Office of Information and Technology said 42 servers were ‘compromised’ and another 25 were deemed ‘suspicious,’ nearly all at the sprawling Geneva and Vienna offices. Three of the ‘compromised’ servers belonged to Human Rights agency, which is located across town from the main U.N. office in Geneva, and two were used by the U.N. Economic Commission for Europe.”

Two points here. If 42 servers were compromised, chances are that 42 servers need to be addressed, at minimum, and that requires a much bigger investment than two weekends of work. The second point is the mention of “across town.” Obviously, the UN’s network connects these two locations, but attacks are oblivious to geographies: if two locations were compromised, then it’s likely the breach spans the entire network!

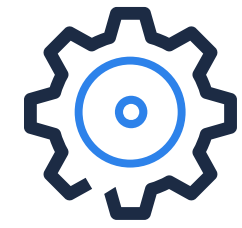
The story takes a slight turn with some of the dramatic statements in the report and interviews. First, the UN clearly indicates that the breach is “state-backed” and the intrusion “definitely looks like espionage.” The reasons for these statements largely lie in the fact that the attackers cleaned up the logs. The officials stated, “There’s not even a trace of a clean-up.”

Cleaning up after an attack is commonplace and certainly does not require state backing or espionage. Here is where the reality of the situation really kicks in. As you can see from the previous statements, the breach is large but under control. However, the officials also stated:

“The leaked Sept. 20 report says logs that would have betrayed the hackers’ activities inside the U.N. networks — what was accessed and what may have been siphoned out — were “cleared.” It also shows that among accounts known to have been accessed were those of domain administrators — who by default have master access to all user accounts in their purview.”

The domain administrators were compromised. There is no way a few weekends of work, 20 servers being rebuilt, and any amount of effort in a month could clean up what a domain administrator may have done to this network. The network will require a deep cleaning, sophisticated forensics, and months of configuration and monitoring to ensure the network and Active Directory are secured.





WHAT COULD HAVE BEEN

⚠ This example, as with so many other government agencies, shows that the breach went all the way to the top. With Active Directory at the core of the identity and access management, not to mention the security hub for the users, groups, data, and computers, the entire enterprise connected to AD is breached.

Here's what could have occurred with the right solution in place:

- Privileged access changes – any change to a privileged group could have been discovered and a real-time alert sent to the IT and security teams. This means that the changes to the Domain Admins group, which is specifically mentioned in the breach, would have been monitored and the change immediately seen.
- Log entries tracked – SIEM solutions are ideal for determining when events occur. SIEMs will gather events as they appear in the log in real time, reducing the effectiveness of clearing the log. If the log is cleared before all entries are obtained, the log being cleared is an entry itself and would trigger an alert for the IT and security teams.
- Privileged attacks – privileged user attacks and persistence are commonplace in Active Directory breaches. The fact that a privileged user can perform actions in Active Directory without causing any log activity is a major issue for most organizations that run AD. Attacks such as DCShadow and DCSync could have been executed without anyone being alerted or any log being generated. It takes a key solution to be able to recognize these attacks and alert the right party. Unfortunately, SIEM solutions fail here, as they only look at the logged events.





WHAT NEEDS TO HAPPEN NOW

⚠ Without the correct solutions in place, much needs to be done to harden this environment's security and to root out the attack. This will require many additional steps and solutions.

First, the computers affected by the attack must be evaluated. This appears to have started given the number of servers being rebuilt. However, with the domain administrators being involved in the attack, any computer on the network could have been involved, including domain controllers and core AD privileges through attacks such as DCSync and DCShadow. After all computers are evaluated, they must be hardened. The hardening might entail rebuilding the computer or evaluating and manually securing all key security areas.

Second, the core security of AD must be evaluated. Unfortunately, this is not a simple command or report that can be run. Deep configurations, complex privilege relationships, and hidden settings need to be unveiled. Solutions such as Alsid for AD perform this task as its core solution. The output is organized as a list of Indicators of Exposure (IoE) with the full backing of the tasks that need to be performed in order to solve the IoE. IoE are highly complex and contain many different settings. [Check the full list of IoE here.](#)

Finally, each of the IoE needs to be continuously monitored for changes or attacks. The fact is that any security setting can be altered as soon as it is made secure, so only a monitoring system can detect changes constantly. The change could occur through a privileged attack, as we've seen, so a standard SIEM is only one of many solutions that needs to be incorporated. Alsid for AD not only shows the IoE for the current environment, but will send an alert if an IoE is altered to a negative, insecure state.





HOT OFF THE PRESS!

The Pentagon is rolling out new cybersecurity standards for the industry starting in 2020. By 2026, all industry contracts will need to meet the requirements. Not much detail is currently available on this new rollout, but we do know there will be five levels, ranging from “basic cyber hygiene” to “very critical technology companies.” (2)

1. Government breaches – can you trust the US Government with your data?, Compaitech, July 24, 2019
2. <https://www.nationaldefensemagazine.org/articles/2020/1/31/pentagon-rolling-out-new-cybersecurity-standards-for-industry>



