Data exfiltration in Latin America

darktrace.com/en/blog/data-exfiltration-in-latin-america/

Max Heinemeyer, Director of Threat Hunting | Tuesday July 20, 2021

Data exfiltration is a popular enterprise for cyber-criminals. All organizations – from government agencies to small businesses – have sensitive data which can be stolen for extortion, competitive advantage, or further inroads in a company's system. It is now the preferred technique of ransomware actors. Some Ransomware-as-a-Service (RaaS) groups have even pioneered a new type of 'extortionware', which focuses solely on data theft without encryption.

Easy money

At a pharmaceutical manufacturing institute in Latin America, Darktrace recently detected the exfiltration of critical files from the company, as this blog will explore.

The organization was an enticing target for two reasons. Firstly, pharmaceutical companies hold a wealth of valuable IP and patient data, which have come under sustained fire this last year as threat actors and nation states infiltrate vaccine research and distribution.

#1
most affected industry for data breaches: pharmaceuticals.

Secondly, Latin America is a treasure trove for cyber-criminals, thanks to huge economic growth in recent years, the digitization of major industries, alongside sub-standard cyber insurance policies and virtually nonexistent regulations.

Even before the COVID-19 pandemic, Brazil and Mexico were in Europol's top ten affected countries. Since then, cases have skyrocketed – and many companies remain underprepared, facing limited support and pressure from government bodies. Strikingly, even though it has suffered estimated losses of almost $8 billion, Brazil still has no data protection law in place.

On top of financial crimes, the LATAM region has been targeted by state-sponsored groups linked to Russia, China, and Iran. Cyber-espionage is used as a method to gain the upper hand in negotiations and advance foreign interests in investment and trade.

Furthermore, as supply chains in the criminal world are hit by the effects of the pandemic, organized crime may begin to leverage the digital world – particularly fraud and phishing – as a possible source of income. La Familia Michoacana, a notorious drug cartel in Mexico, has reportedly begun enlisting Dark Web hackers.

Despite the number of threats facing Latin America, organizations have been slow to adopt defensive technology. So when the attacker in the case below chose a small organization in the LATAM region, they probably expected to face only signature-based, legacy security tools. Sensing that this would be easy prey – with little resistance and large profit to be made – the actor launched their first steps.

How the intrusion played out

During a Proof of Value trial with the company, Darktrace detected unusual activity from a server, following external remote connectivity.


Figure 1: Timeline of the attack.

The attack began when an internal server received an unusual connection over RDP from an external IP. The connection lasted five hours. The external IP then established a new SMB session to the same server using administrative credentials. The external IP leveraged SMB to access a file, which appeared to contain unencrypted passwords.


65%
of the Colombian population now use the Internet, compared to only 3% in 2000.

From there, the external IP downloaded over 18,000 files over SMB. Based on the file names, it appears that the data was highly sensitive. In total, the external IP downloaded around 150 MB of data from the internal server.

Unusual activity post remote connections

Self-Learning AI detected that the IP address was 100% rare for the organization and server. The data transfer was also detected as unusual for the device's 'pattern of life'. Unfortunately, as Antigena was being trialled in passive mode, Darktrace could not intervene and disrupt the attack.

Nevertheless, Darktrace fired a number of high-confidence alerts to warn the security team. The figure below shows five-day activity from an example device in the same situation, with a high volume of clustered alerts. These reflect the unusual increase in volume transferred externally from a breach device.

Figure 2: A similar device received an incoming remote desktop connection, highlighted by the first model breach (orange dot). Shortly after, the external device accessed an unencrypted password file. At the same time, the device transferred an unusual volume of data to a rare external source IP.

Data exfiltration methods: RDP and password file access

The threat actor managed to bypass all the other existing security products in the company. They did this with legitimate administrative credentials, which were used to establish the RDP and SMB connections. RDP credentials are easily bought off the Dark Web and have proved a popular form of initial access, especially this year as employees continue to work remotely.

In addition, improper password management can unlock an organization's digital kingdom. One of the accessed files was a password file, enabling the actor to quickly escalate privileges. After this point, only an AI-powered defensive tool could keep up with the speed of the intrusion.

Leveraging common protocols such as SMB to exfiltrate data is a common tactic. Internet-exposed servers are still a major risk to organizations as attackers exploit open and unused ports.

Moreover, the files transferred during the activity were saved as receipts with the names of partners and customers. This is extremely dangerous and could have put the company's reputation at serious risk. Luckily, Self-Learning AI detected the malicious actions and warned the security team immediately, allowing them to stop further exfiltration and any follow-up activity.

Protecting sensitive data

The example above demonstrates that even the smallest of companies can fall victim to an attack. Small and medium-sized enterprises are targeted because they own important data and IP, yet often lack robust security and resources. This makes them simple catches compared to large establishments or governments.

Darktrace's AI has the ability to detect malicious data exfiltration from subtle changes in behavior. In this case, the targeted server regularly transfers data in and out of the organization, yet Darktrace scored the incoming external IP with the highest rarity. In other words, Darktrace considered the data transfer activity highly unusual and outside of the server's normal 'pattern of life'.

This enabled the security team to respond to the threat and take the server offline for further investigation. If Darktrace Antigena had been active in the environment, it would have responded seconds after the initial compromise, stopping the threat at machine speed.

Thanks to Darktrace analyst Kendra Gonzalez Duran for her insights on the above threat find.

Learn how to defend your company from data exfiltration and malicious insiders

Darktrace model detections:

- Compliance / Incoming Remote Desktop
- Compliance / Possible Unencrypted Password File On Server
- Anomalous Connection/ Data Sent to Rare Domain

MITRE ATT&CK techniques observed:

Initial Access	T1078 – Valid Accounts
Credential access	T1552.001 – Unsecured Credentials: Credentials In Files
Exfiltration	T1048.003 – Exfiltrate Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

Max Heinemeyer

Max is a cyber security expert with over a decade of experience in the field, specializing in a wide range of areas such as Penetration Testing, Red-Teaming, SIEM and SOC consulting and hunting Advanced Persistent Threat (APT) groups. At Darktrace, Max oversees global threat hunting efforts, working with strategic customers to investigate and respond to cyber-threats. He works closely with the R&D team at Darktrace's Cambridge UK headquarters, leading research into new AI innovations and their various defensive and offensive applications. Max's insights are regularly featured in international media outlets such as the

BBC, Forbes and WIRED. When living in Germany, he was an active member of the Chaos Computer Club. Max holds an MSc from the University of Duisburg-Essen and a BSc from the Cooperative State University Stuttgart in International Business Information Systems.