Journal of Corporate Governance, Insurance, and Risk Management
https://www.acadlore.com/journals/JCGIRM

Cyber Attack Against E-Albania and Its Social, Economic and Strategic Effects

Aleksander Biberaj[1*], Enida Sheme[2], Alban Rakipi[1], Sonila Xhaferllari[1], Renalda Kushe[1], Mirjeta Alinci[1]

[1] Department of Electronics and Telecommunication, Faculty of Information Technology, Polytechnic University of Tirana, Mother Teresa Square Nr. 4, 1001 Tirana, Albania
[2] Department of Computer, Faculty of Information Technology, Polytechnic University of Tirana, Mother Teresa Square Nr. 4, 1001 Tirana, Albania

[*] Correspondence: Aleksander Biberaj (abiberaj@fti.edu.al)

Received: 09-06-2022 **Revised:** 10-28-2022 **Accepted:** 11-13-2022

Citation: Biberaj, A., Sheme, E., Rakipi, A., Xhaferllari, S., Kushe, R., & Alinci, M. (2022). Cyber attack against E-Albania and its social, economic and strategic effects. *J. Corp. Gov. Insur. Risk Manag.*, *9*(2), 341-347. https://doi.org/10.56578/jcgirm090204.

Abstract: Purpose: During last years, even because of pandemic situation caused by covid-19 virus, in Albania most of governmental public services for citizens, businesses and other customers were offered in an electronic way by creating a national database (e-Albania), offering more than 2200 services. As this electronic system was newly implemented, time after time it was attacked from hackers in different sectors of services, causing the interruption of service for hours, downloading all the confidential information and publishing them. After several partial attacks, in July 2022 came the general attack of the whole system, which black out the system and services for several days. Cyber actors - identifying as "HomeLand Justice" - launched a destructive cyber-attack against e-Albania which rendered websites and services unavailable. An investigation indicates cyber actors acquired initial access to the victim's network approximately 14 months before launching the destructive cyber-attack, which included a ransomware-style file encryptor and disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content. From late July to mid-August 2022, social media accounts associated with HomeLand Justice demonstrated a repeated pattern of advertising Albanian Government information for release, posting a poll asking respondents to select the government information to be released by HomeLand Justice, and then releasing that information - either in a .zip file or a video of a screen recording with the documents shown. This cyber-attack creates social problems, economical loss and influenced negatively in the reputation of e-Albania and damage as well strategically the country and development of this sector in the future. **Methodology:** We have monitored the system and the attack, and we continue to do this. We analyze and synthesis the data collected, to come to conclusions and recommendations needed for the future. All the data which we have used are open for public, and mostly are primary data. The research method combines both quantitative and qualitative methods, but it is closer with qualitative method, as far as there in not enough data for using e pure quantitative analysis. We have used mostly the descriptive method. **Results/Findings:** Improving essentially the cyber infrastructure to avoid in the future such attacks with high social, economic and strategical cost. **Conclusions:** In the institution there was not a team for Cyber Security Monitoring the system, so called SOC (Security Operation Center), who controls in the real time all the logins. It was missing as well so called "Identifying Behavior". There was not e separation of active directory, in physic machines and virtual machines, they were altogether. As the administrator had Full Right Privilege, the hacker doesn't need to create a Privilege Escalation Vertical, so he easily took all the right of Admin. **Originality and Practical Implications:** The paper is original; it has not been previously published and it is not under consideration by any other publisher. The originality of the method stands in the fact that it is the first case in the world in information age, that a country (a whole electronic system, e-Albania), face a such complex, well organized and hard cyber-attack, which collapse the system for several days. All the data are authentic ones.

Keywords: Artificial intelligence; E-Albania; Electronic attack; Cyber security; Data base; HomeLand justice; Pattern behavior; Traffics malware

1. Introduction

In July 2022, the attackers identifying as "HomeLand Justice" - launched a destructive cyber-attack against e-Albania, which rendered websites and services unavailable. An investigation indicates that cyber actors acquired initial access to the victim's network approximately 14 months before launching the destructive cyber-attack, which included a ransomware-style file encryptor and disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content. In June 2022, HomeLand Justice created a website and multiple social media profiles. On July 18, 2022, HomeLand Justice claimed credit for the cyber-attack on e-Albania infrastructure. On July 23, 2022, Homeland Justice posted videos of the cyber-attack on their website. From late July to mid-August 2022, social media accounts associated with HomeLand Justice demonstrated a repeated pattern of advertising Albanian Government information for release, posting a poll asking respondents to select the government information to be released by HomeL and Justice, and then releasing that information - either in a .zip file or a video of a screen recording with the documents shown.

2. Literature Review

There are lot of technical literatures about cyber-attacks, but it is too difficult when we talk about the specific case, as these issues are very sensitive and confidential ones. Even in this cyber-attack against e-Albania it was very difficult to get the proper information because every information was confidential one. There were produced reports from different national governmental agencies and international agencies, as well from different companies offered to e- Albania as out-sources, but all these reports remind very confidential.

2.1 Technical Details

Approximately 14 months before encryption and wiper attacks initial access was obtained via exploitation of an Internet-facing Microsoft SharePoint, exploiting CVE-2019-0604. After obtaining access to the victim environment, the actors used several .aspx webshells, pickers.aspx, error4.aspx, ClientBin.aspx, to maintain persistence. During this timeframe, the actors also used RDP (primarily), SMB, and FTP for lateral movement throughout the victim environment. Persistence in cybersecurity occurs when a threat actor discreetly maintains long-term access to systems despite disruptions such as restarts or changed credentials. Bad actors can place an implant or a "stub" that both evades automated antivirus solutions and kickstarts more malware. This malware is usually hidden in legitimate startup folders or within scheduled tasks and services, making it harder to find.

After you reboot your system or log off and on again, the stub or malware is retriggered to run again. In other words, persistence enables hackers who gain access into your environments to keep it—oftentimes without you knowing they have access in the first place (Vlsaggio & Blasio, 2010).

The actors used a compromised Microsoft Exchange account to run searches (via CmdLets New-MailboxSearch and Get-Recipient) on various mailboxes, including for administrator accounts. In this timeframe, the actors used the compromised account to create a new Exchange account and add it to the Organization Management role group. They made thousands of HTTP POST requests to Exchange servers of the victim organization. The FBI observed the client transferring roughly 70-160 MB of data, and the server transferring roughly 3-20 GB of data.

Clients mostly are working in a narrow bandwidth for their own needs, while servers are processing a huge data base coming from different customers and entities, and operating with a large bandwidth. In this context the authors were much more interested to transfer big data from the centralized servers than from peripheric servers of the customers. Approximately twelve months after initial access and two months before launching the destructive cyber-attack, the actors made connections to IP addresses belonging to the victim organization's Virtual Private Network (VPN) appliance. The actors' activity primarily involved two compromised accounts. The actors executed the "Advanced Port Scanner" (advanced_port_scanner.exe). There was also found evidence of Mimikatz usage and LSASS dumping.

For the encryption component of the cyber-attack, the actor logged in to a victim organization print server via RDP and kicked off a process (Mellona.exe) which would propagate the GoXml.exe encryptor to a list of internal machines, along with a persistence script called win.bat. As deployed, GoXML.exe encrypted all files (except those having extensions .exe, .dll, .sys, .lnk, or. lck) on the target system, leaving behind a ransom note titled How_To_Unlock_MyFiles.txt in each folder impacted.

In the same timeframe as the encryption attack, the actors began actions that resulted in raw disk drives being wiped with the Disk Wiper tool (cl.exe). Approximately over the next eight hours, numerous RDP connections were logged from an identified victim server to other hosts on the victim's network. Command line execution of cl.exe was observed in cached bitmap files from these RDP sessions on the victim server (Namitha & Keerthijith, 2018).

The same attack that happened in governmental infrastructures, happen 2 weeks ago in Albanian State Police Infrastructures, especially in TIMS infrastructure. Total Information Management System (TIMS) - The USG

aided implement within the ASP a sustainable, modern, and integrated, information management system toenhance capabilities in criminal investigation, case management, criminal intelligence analysis, border control and overall police administration.

This system is a closed system and the reason that this system and other systems of ASP were attacked was because all these systems were in the same domain with Microsoft Exchange infrastructure, which in this case also was used for the attack. It was discussed among the specialist and debated with decision making (highest level of politics), about the system, to be closed or open, centralized, or de-centralized. While the IT specialist propose for a decentralized system (open system) the politics decides for centralized system (closed one). Having a big data system centralized, being in the same domain, had a high risk because of the hacking the system, as it happened during the cyber-attack. The system was attack in the main domain, which collapse e-Albania as a whole system.

If the system would have been de-centralized, the situation may have been different in positive aspects, being more protected from the attack.

To overcome the situation and investigate about it, there are several actors involved. We can mention Microsoft DART, that immediately sent the team in Albania to help solve the issues, NATO team was also present to help and give their support and expertise. Related to the investigation, it is still ongoing by the Persecutor and Cyber Unit (part of ASP) and since the beginning the FBI has also been presented to investigate and help Albanian authorities. They also have made a detailed report about what has happened this case. John Group International was also present with their Cyber Team.

Initial access

Timeframe: Approximately 14 months before encryption and wiper attacks.

Details: Initial access was obtained via exploitation of an Internet-facing Microsoft SharePoint, exploiting CVE-2019-0604.

Persistence and Lateral movement

Timeframe: Approximately several days to two months after initial compromise.

Details: After obtaining access to the victim environment, the actors used several .aspx webshells, pickers.aspx, error4.aspx, and ClientBin.aspx, to maintain persistence. During this timeframe, the actors also used RDP (primarily), SMB, and FTP for lateral movement throughout the victim environment.

Exchange Server compromise

Timeframe: Approximately 1-6 months after initial compromise.

Details: The actors used a compromised Microsoft Exchange account to run searches (via CmdLets New-MailboxSearch and Get-Recipient) on various mailboxes, including for administrator accounts. In this timeframe, the actors used the compromised account to create a new Exchange account and add it to the Organization Management role group.

Likely Email exfiltration

Timeframe: Approximately 8 months after initial compromise.

Details: The actors made thousands of HTTP POST requests to Exchange servers of the victim organization. The FBI observed the client transferring roughly 70-160 MB of data, and the server transferring roughly 3-20 GB of data.

VPN activity

Timeframe: Approximately 12-14 months after initial compromise.

Details: Approximately twelve months after initial access and two months before launching the destructive cyber attack, the actors made connections to IP addresses belonging to the victim organization's Virtual Private Network (VPN) appliance. The actors' activity primarily involved two compromised accounts. The actors executed the "Advanced Port Scanner" (advanced_port_scanner.exe). The FBI also found evidence of Mimikatz usage and LSASS dumping.

File Cryptor (ransomware-style file encryptor)

Timeframe: Approximately 14 months after initial compromise.

Details: For the encryption component of the cyber-attack, the actor logged in to a victim organization print server via RDP and kicked off a process (Mellona.exe) which would propagate the GoXml.exe encryptor to a list of internal machines, along with a persistence script called win.bat. As deployed, GoXML.exe encrypted all files (except those having extensions .exe, .dll, .sys, .lnk, or .lck) on the target system, leaving behind a ransom note titled How_To_Unlock_MyFiles.txt in each folder impacted.

Wiper attack

Timeframe: Approximately 14 months after initial compromise.

Details: In the same timeframe as the encryption attack, the actors began actions that resulted in raw disk drives being wiped with the Disk Wiper tool (cl.exe) described in Appendix A. Approximately over the next eight hours, numerous RDP connections were logged from an identified victim server to other hosts on the victim's network (CISA, 2022).

Command line execution of cl.exe was observed in cached bitmap files from these RDP sessions on the victim server.

2.2 Mitigations

It is recommended organizations apply the following best practices to reduce risk of compromise:

- **Ensure anti-virus and anti-malware software is enabled and signature definitions are updated** regularly and in a timely manner. Well-maintained anti-virus software may prevent use of commonly deployed cyber attacker tools that are delivered via spear-phishing.
- **Adopt threat reputation services at the network device, operating system, application, and email service levels**. Reputation services can be used to detect or prevent low-reputation email addresses, files, URLs, and IP addresses used in spear-phishing attacks.
- If your organization is employing certain types of software and appliances vulnerable to known Common Vulnerabilities and Exposures (CVEs), **ensure those vulnerabilities are patched**. Prioritize patching known exploited vulnerabilities.
- **Monitor for unusually large amounts of data** (i.e., several GB) being transferred from a Microsoft Exchange server.
- **Check the host-based indications**, including webshells, for positive hits within your environment.
- **Maintain and test** an incident response plan.
- **Ensure your organization has a vulnerability management program** in place and that it prioritizes patch management and vulnerability scanning of known exploited vulnerabilities. **Note**: CISA's Cyber Hygiene Services (CyHy) are free to all state, local, tribal, and territorial (SLTT) organizations, as well as public and private sector critical infrastructure organizations.
- **Properly configure and secure** internet-facing network devices.
    - Do not expose management interfaces to the internet.
    - Disable unused or unnecessary network ports and protocols.
    - Disable/remove unused network services and devices.
- **Adopt zero-trust principles and architecture**, including:
    - Micro-segmenting networks and functions to limit or block lateral movements.
    - Enforcing phishing-resistant multifactor authentication (MFA) for all users and VPN connections.
    - Restricting access to trusted devices and users on the networks.

3. Research Methodology

We have monitored the system to understand what happened, and to prevent happening again in the future. We have analyzed and synthesis the facts, for concluding and recommended what is needed in order our data and the national network to be protected and secure.

3.1 Data Collection

During the period of October 2021 - January 2022, the threat actors used a unique email exfiltration tool which interacted with the Exchange web services APIs to collect email in a manner that masked the actions. Data exfiltration by using email exfiltration, is a malicious process whereby cybercriminals (external actors) or insiders (employees, contractors, and third-party suppliers), accidentally or deliberately steal or move data from inside to outside a company's perimeter without authorization. Of course, this manner is very effective comparing with the ordinary tools, because while it seems to be very simple, it is a very sophisticated manner because it masks the action of hacking, and it is not easy to be recognized from the Cyber Security Monitoring called SOC (Security Operation Center).

The threat actors accomplished these actions by creating an identity named "HealthMailbox55x2yq" to mimic a Microsoft Exchange Health Manager Service account using Exchange PowerShell commands on the Exchange Servers. The threat actors then added the account to the highly privileged exchange built-in role group "Organization Management" to later add the role of "Application Impersonation". The Application Impersonation management role enables applications to impersonate users in an organization to perform tasks on behalf of the user, providing the ability for the application to act as the owner of a mailbox (Microsoft, 2022).

3.2 Defense Evasion

Prior to launching the final stage of the attack, the threat actors gained administrative access to a deployed endpoint detection and response (EDR) solution to make modifications, removing libraries that affected the agents across the enterprise. In addition, a binary to disable components of Microsoft Defender Antivirus was propagated using custom tooling. The distributed binary named *disable-defender.exe* queries for TokenElevation using the GetTokenInformation API and checks if the process is running with elevated privileges. If the token is not running

with elevated privilege, the binary prints “Must run as admin!\n”. If the token is elevated, it queries TokenUser and checks if the SID is “S-1-5-18”. If the current process doesn’t run under system context, it prints “Restarting with privileges\n” and attempts to elevate the privilege (Hu & Hancke, 2017).

To elevate the privilege, the binary checks if the TrustedInstaller service is enabled. To do this, it starts the service “SeDebugPrivilege” and “SeImpersonatePrivilege” to assign privileges to itself. It then looks for *winlogon.exe* process, acquires its token, and impersonates calling thread using ImpersonateLoggedOnUser/SetThreadToken. Organizations can take a significant step toward reducing the risk of token theft by ensuring that they have full visibility of where and how their users are authenticating. To access critical applications like Exchange Online or SharePoint, the device used should be known by the organization. Utilizing compliance tools like Intune in combination with device based conditional access policies can help to keep devices up to date with patches, antivirus definitions, and EDR solutions. Allowing only known devices that adhere to Microsoft’s recommended security baselines helps mitigate the risk of commodity credential theft malware being able to compromise end user devices. After impersonating as *winlogon.exe*, it opens TrustedInstaller process, acquires its token for impersonation and creates a new process with elevated privileges using CreateProcessWithTokenW, as it is shown in Figure 1 below.

Figure 1. How the attacker can evade defense components

Once it successfully creates its own process with TrustedInstaller privilege, it proceeds to disable Defender components. Microsoft 365 Defender is an eXtended detection and response (XDR) solution that automatically collects, correlates, and analyzes signal, threat, and alert data from *across* your Microsoft 365 environment, including *endpoint, email, applications, and identities*. It leverages artificial intelligence (AI) and automation to *automatically* stop attacks and remediate affected assets into a safe state. XDR is the next step in security, unifying endpoint (endpoint detection and response or EDR), email, app, and identity security in one place. The actors were able to make disable the Defender Components, which leave the system without protection as it happened (Calzavara et al., 2019).

They acted as follows:

- Terminates smartscreen.exe
- Modifies WinDefend service to DemandLoad.
- Modifies “TamperProtection” value to 0
- Queries WMI “Root\Microsoft\Windows\Defender” Namespace “MSFT_MpPreference” class for “DisableRealtimeMonitoring”
- Sets “DisableAntiSpyware” value to 1
- Sets “SecurityHealth” value to 3
- Sets “DisableAntiSpyware” value to 0
- Sets “SYSTEM\CurrentControlSet\Services\WinDefend” service “Start” value to 3
- Sets “DisableRealtimeMonitoring” value to 1
- Modifies further settings using WMI “Root\Microsoft\Windows\Defender” Namespace “MSFT_MpPreference” class values,
    - “EnableControlledFolderAccess”
    - “PUAProtection”
    - “DisableRealtimeMonitoring”
    - “DisableBehaviorMonitoring”
    - “DisableBlockAtFirstSeen”
    - “DisablePrivacyMode”
    - “SignatureDisableUpdateOnStartupWithoutEngine”
    - “DisableArchiveScanning”
    - “DisableIntrusionPreventionSystem”
    - “DisableScriptScanning”
    - “DisableAntiSpyware”
    - “DisableAntiVirus”
    - “SubmitSamplesConsent”
    - “MAPSReporting”
    - “HighThreatDefaultAction”

- "ModerateThreatDefaultAction"
- "LowThreatDefaultAction"
- "SevereThreatDefaultAction"
- "ScanScheduleDay"

Additional evasion techniques included the deletion of tooling, Windows events, and application logs (Prapty et al., 2020).

3.3 Social, Economic and Strategic Effects of the Attack

This hard attack may cause:

a) social problems because all the confidential data of the citizens were published, as the private home addresses, telephone numbers, their properties (lands, homes, cars), salaries/incomes, etc.

b) economic problems for the businesses, banking system, financial market, insurance companies, etc.

In the time of reviewing this article two banks were subject of hacking, which almost cause a crash in these banks, regardless the attack was not published from the Government or Central Bank of Albania, or even banks itself, which may cause a panic to the customers and collapsing the banking system.

d) strategic problems as Albania is NATO member and EU candidate for membership.

4. Conclusions

1. The attack against e-Albania came through a PDF document to the administrator of the system, who download the document, which opened a port RDP (Remote Desktop Protocol) and create a free access in distance for the hacker. As the administrator had "Full Privilege" the hacker accessed the whole "Enterprise Admin." of the domain and then delete all the "Virtual Machines".

There were reasons happening this:

a) Unfortunately, in the institution there was not a team for Cyber Security Monitoring the system called SOC (Security Operation Center), who controls in the real time all the logins in regime (24 hours/Day, 7 Days/Week). SOC together with IRT (Incident Response Team) monitor everything in the system, to protect the system and to act immediately against the attack.

b) It was missing so called "Identifying Behavior". Traffics Malware may be identified by two manners, by so called 1. "Signatures", which is an overcome method from the hackers, and by 2. "Artificial Intelligence", which operates with Pattern Behavior. As Signature may be cloned, "Pattern Behavior" monitor the system, and if it recognizes strange behavior, immediately gives the alarm, through so called IDR and XDR (which may be implemented by Microsoft, Palo Alto, etc.).

c) There was not e separation of active directory, in physic machines and virtual machines, they were altogether.

d) As the administrator had Full Right Privilege, the hacker doesn't need to create a Privilege Escalation Vertical, so he easily took all the right of Admin.

5. Recommendation

As the hacker attacks all the business (focusing on the finance system, banking system, insurance companies) and all the personal data of citizens in Albania, we must:

1. Invest largely in the technological infrastructure, as so far it is missing.
2. Invest in know-how, to prepare skilled people and professionals for cyber security, and to pay them well.
3. Create training centers for cyber security specialists, in cooperation with universities, with joining programs with professional and business institutions/academies, as EC Councill.
4. Implement the General Data Protection Right (GDPR), as it is as well a condition for EU accession.
5. Open new programs at universities focusing in cyber security and improving existing colliculus for IT engineers/specialists.

Data availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of interest

The authors declare that they have no conflicts of interest.

References

Calzavara, S., Rabitti, A., & Bugliesi, M. (2019). Sub-session hijacking on the web: Root causes and prevention. *J Comput. Secur.*, *27*(2), 233-257. https://doi.org/10.3233/JCS-181149.

Hu, Q. & Hancke, G. P. (2017). A session hijacking attack on physical layer key generation agreement, In 2017 IEEE International Conference on Industrial Technology. (ICIT). Toronto, ON, Canada, 22-25 March 2017. IEEE. pp. 1418-1423. https://doi.org/10.1109/ICIT.2017.7915573.

Iranian State Actors Conduct Cyber Operations Against the Government of Albania. CISA, (2022). https://www.cisa.gov/uscert/ncas/alerts/aa22-264a#:~:text=In%20July%202022%2C%20Iranian%20state,rendered%20websites%20and%20services%20unavailable.

Microsoft investigates Iranian attacks against the Albanian government. Microsoft, (2022). https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

Namitha, P. & Keerthijith, P. (2018). A Survey on Session Management Vulnerabilities in Web Application, In 2018 International Conference on Control, Power, Communication and Computing Technologies. (ICCPCCT). Kannur, India, 23-24 March 2018. IEEE. pp. 528-532. https://doi.org/10.1109/ICCPCCT.2018.8574238.

Prapty, R. T., Md, S. A., Hossain, S., & Narman, H. S. (2020). Preventing session hijacking using encrypted one-time-cookies, In 2020 Wireless Telecommunications Symposium. (WTS). Washington, DC, USA, 22-24 April 2020. IEEE. pp. 1-6. https://doi.org/10.1109/WTS48268.2020.9198717.

Vlsaggio, C. A. & Blasio, L. C. (2010). Session management vulnerabilities in today's web. *IEEE Secur. Priv.*, *8*(5), 48-56. https://doi.org/10.1109/MSP.2010.114.