HS

Health Sector

Research Report

MARCH

2024

XG3 UNIT

xMDR

powered by Cipher

Introduction

Accelerated digitalisation in the healthcare sector has brought numerous benefits, but it has also exposed institutions to a growing threat: cyber attacks. The interconnectedness of systems and the vast amount of medical data stored electronically have made the sector a **frequent target of cyber attacks**. The magnitude of the problem is evidenced by reports documenting incidents of data breaches in the health sector, where sensitive medical information becomes currency in cyberspace. These attacks compromise the integrity and confidentiality of patient data, with **highly damaging medical and financial consequences**.

Within this challenging environment, the **x63Unit**, a specialized multidisciplinary unit in cyber intelligence, stands as a pioneering force, moving beyond conventional security approaches. The primary aim of the x63Unit is to gain an exhaustive understanding of the digital adversary, scrutinizing their identity, the tools they utilize, the vulnerabilities they exploit, and their operational tactics. This multifaceted perspective fosters the development of forward-thinking defense strategies, empowering the anticipation and proactive prevention of potential cyber incidents.

Building on this foundation, the **xMDR platform** emerges as an innovative solution that encapsulates the extensive expertise of the **x63Unit**. It serves as a nexus where the comprehensive knowledge and diverse insights of this multidisciplinary unit are translated into practical, ready-to-use defenses. Customized to the unique environments of each client.

The leakage of personal data, medical records and other confidential information not only violates the privacy of individuals, but also impacts patient confidence and generates significant financial consequences. The average cost of a data breach in the healthcare sector is about $11 million, covering direct costs such as data recovery, notification of affected individuals and enhanced security measures, as well as indirect losses associated with decreased patient confidence, potential lawsuits and disruption to normal operations.

For 13 consecutive years, the healthcare sector has reported **the most costly data breaches**, averaging USD 10.93 million per incident. By 2023, an estimated 40 million patients are estimated to have been affected by data breaches, indicating a possible record for this year.

The European Union (EU) healthcare system is also facing a **growing threat from cyber-attacks**. A number of cybersecurity incidents compromising confidential hospital information and patient data have been reported during 2023. The European Union Cybersecurity Agency's (ENISA) Healthcare Data Breaches report reveals that 53% of cyber incidents targeted healthcare providers, with **hospitals being the main targets**.

Two of this year's notable attacks were against Managed North Care of America (MCNA), led by **LockBit**, which affected 8,923,662 people and demanded a ransom of $10 million, and against the Hospital Clínic de Barcelona, which was carried out by **Ransom House**, compromising 4.5 terabytes of data and demanding $4.5 million in ransom.

Ransomware in healthcare

Within ransomware, the most prominent players in 2023 are Lockbit, RansomHouse and Blackcat, each for different reasons according to research by **x63Unit**.

RansomHouse, active since December 2021, targets primarily the health sector, evident from its attacks in Colombia and Spain. Despite denying ransomware use, their presence on the Dark Web contradicts this claim. This group, potentially comprising cybersecurity experts, emphasizes mediation aiming to minimize harm, preferring negotiations to conflicts, displaying an inclination towards cooperation and conflict resolution

Their interest in the health sector could be due to a desire to expose the lack of security of particularly sensitive data.

Lockbit would be the main player to watch out for, as due to its size and high operability, it is the most persistent threat. Lockbit is one of the most profiling groups in cybercrime. In addition to its longevity and long-standing membership system, it is constantly innovating technically and logistically, making it the most mature group in existence.

Blackcat group, noted for its grey morality, could be considered the main threat of interest, as its techniques tend to be highly damaging, as was the case with the publication of compromised photographs of oncology patients in its attack against Lehigh Valley Health Network. The creators of BlackCat ransomware offer their services under a ransomware-as-a-service strategy.

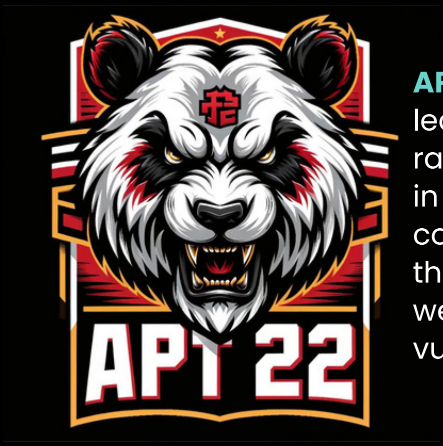
It uses a cryptor written in Rust to attack Windows and Linux environments. It uses tools such as Fendr to extract data, indicating possible links to BlackMatter. In addition, it uses PsExec, Mimikatz and Nirsoft to move laterally and obtain passwords.

APT in healthcare

Attacks by APT groups tend to be highly advanced, are often motivated by espionage, and their primary mission is often to extract sensitive information according to research by **x63Unit**.

FIN8, active since 2016, focuses on financially motivated cyber operations in various sectors. It compromises point-of-sale (POS) systems using malware such as PUNCHTRACK and BADHATCH to steal payment card data. Although it does not have a genuine interest in the healthcare sector, it has been observed to be a target, as there have been occasions when a campaign has been directed against this specific sector.

APT41, with origins suspected in Chengdu, China, has a track record of targeting the health sector through state-sponsored espionage and digital extortion activities. Believed to be associated with China's Ministry of State Security, APT41 has engaged in cyber operations dating back to at least 2007. Operating globally, the group has directly targeted organizations in numerous countries, focusing on healthcare entities, including pharmaceuticals, in its espionage campaigns.



APT22 is likely linked to China and has been active since at least early 2014, engaging in intrusions and attacks against a range of public and private sector entities. Their targets extend in the United States, Europe, and East Asia. The group has conducted prolonged targeting of health centers, specifically those focused on cancer research. APT22 employs strategic web compromises to passively exploit targets, identifying vulnerable public-facing web servers within victim networks.

Hacktivism in healthcare

Hacktivist groups have also focused on the health sector, mainly on DDoS-type attacks, which, however, can be very disruptive when it comes to disturb critical services. In this aspect, the **x63unit** monitors and pays close attention to the activities of these groups, integrating into their main communication channels to anticipate possible attacks.

Killnet, a pro-Russian hacktivist group, gained notoriety during the Russia-Ukraine conflict for unsophisticated but widespread DDoS attacks and misinformation campaigns. Killnet, now rebranded as 'Black Skills,' is categorized as a "private military hacking company" despite low credibility, serving as a model for paid "hackers for hire." Merging with lesser groups enhances their attack effectiveness, creating ambiguity in attribution.

Killnet remains a legitimate threat due to its persistent use of DDoS attacks, manipulating cognitive perceptions and war narratives through media exposure and propaganda.

Anonymous Sudan, a rapidly growing hacktivist group, identifies as Sudanese and operates with religious and political motivations. Since January 2023, they have executed over 670 distributed denial-of-service (DoS) attacks, aiming to defend Islam against Western nations. Anonymous Sudan's targets span multiple countries, impacting critical infrastructure and global sectors. The group employs a "blitz" approach, concentrating attacks on various interfaces.

**Lapsus$** was a transnational group of threat actors predominantly based in the United Kingdom (UK) and Brazil, which emerged as a result of the merger of two previous cybercriminal groups, Cyberteam and Recursion Team. It was officially identified between September and December 2021. Although it is currently inactive, there is uncertainty that its members may limit their public profile, join other groups or rebrand. Operating in a dynamic threat ecosystem, Lapsus$ demonstrated different approaches to targeting, credential theft, and direct interaction with the public.

IAB's in healthcare

The IABs, or Initial Access Brokers, that we will discuss are a **direct result of the proprietary investigations conducted by the x63Unit**. These actors specialize in selling access to companies, thereby facilitating other malicious actors to execute their attacks. Presented below are the most pertinent IABs for the healthcare sector, as identified in the underground networks. All the information provided here is sourced from the **x63Unit's Digital Adversary** platform, showcasing their in-depth research and expertise in the field.

Sapphire Cosmos Taurus: It is only by the Russian community Exploit.in. It recently sold RDP access to a US dental clinic in auction mode starting at $500. Historically, he has been exclusively dedicated to selling access from various countries outside the CIS zone, mainly located in Europe and the United States. It has specialised in providing its customers with RDP access to victims' intranets. Has had occasional sales focused on PII data exfiltrated from third parties

It has had a customer relationship in the past with other actors specialising in pentesting and reconnaissance software programming.

Olive Cosmos Taurus: Mainly runs on XSS.is and communicates in Russian. Recently it offered RDP access with user privileges to a UK company in the pharmaceutical industry whose anti-virus was ESET.

Historically its activity has been very varied, with no clear pattern. Apart from selling access, he has published streaming service credentials and PII information. The actor has shown interest in the past in vulnerabilities related to Citrix (CVE-2023-4966).

He has been observed sharing information about RDP brute-force attacks against cloud services, such as Amazon.

Teal Cosmos Taurus: Moved mainly by Exploit.in. Sells access to a UK-based cancer research company. Sells in bidding format, starting at $500. His track record is varied and the type of access he tends to sell specialises in web consoles and access to hosting administration panels (Cpanels). His main victims are based in Indonesia, the United States, France, Japan and the United Kingdom, among others. He has been active in discussions on how to get started in the world of pentesting, in the search for and development of reconnaissance and scraping tools, and in operational security (OPSEC).

Leaks vendors in healthcare

A leak vendor is an actor dedicated to the unauthorized disclosure of confidential information, the following actors stems from the **x63Unit's** own research. In the realm of cybersecurity and information, leakers often access sensitive or secret data, such as corporate documents, personal data, and internal communications, and then proceed to make them public. This comprehensive information about leak vendors, derived from the investigative efforts of the **x63Unit**, is available on the **xMDR Digital Adversary** platform, demonstrating the unit's commitment to uncovering and understanding these specific cyber threats.

Jade Cosmos Taurus: Offers a DB of 100k records for a hospital in Thailand. The actor is mainly active on forums such as CrackedTo.

He maintains a very varied profile, without being specifically dedicated to any particular activity. The assets he offers vary from access credentials to customer accounts of streaming and entertainment platforms such as Netflix, to exfiltrated databases, possibly by third parties.

Violet Cosmos Taurus: Sale of the complete DB of a hospital in Vietnam with PII. Moved mainly by Breachforums. This player is mostly focused on the supply of exfiltrated databases, possibly by third parties. It also has activities related to the sale of logs in Combolist format. Its target geographies are varied, but there seems to be a slight preference for victims located in Asia, such as Japan, China and Indonesia.

It has been observed in some trivial conversations with other more well-known Spanish-speaking actors, which recently offered to sell a database belonging to the municipality of Villamayor, Salamanca, Spain.

Bronze Cosmos Taurus: Sells 27GB of DB from psmmc.med.sa. Moves mainly through Breachforums. The actor might have had a hacktivist motivation in his early days, as virtually all of his targets were against Saudi Arabia. He has recently created his own Telegram channel which he uses to advertise his victims and new movements, advertising a range of international targets geographically, which could mean a more economical positioning compared to his beginnings.

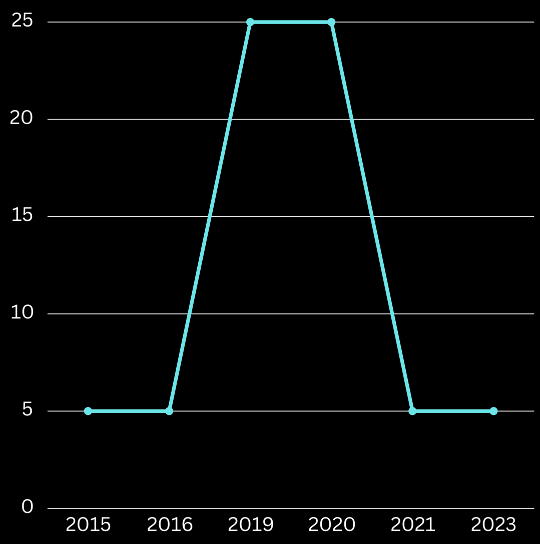
It is currently recruiting network-team and pentesting profiles to carry out intrusions to exfiltrate data for its new marketplace, which it plans to launch soon.

Tools & CVE's

• CVE's related to actors

According to data from the **xMDR Platform, from a pool of 90755 CVEs registered**, the different vulnerabilities that have been associated with attacks on the health sector over the last few years have been observed. The exploitation of these vulnerabilities by the actors allows them to carry out the attack, and is therefore a field of study of interest for the prevention of such attacks. It is possible to observe that vulnerabilities from previous years are being exploited, so the lack of updating them is an important risk factor to take into consideration.

- CVE-2016-0051
- CVE-2023-33466
- CVE-2020-11022
- CVE-2020-11023
- CVE-2015-9251
- CVE-2019-11358
- CVE-2020-0601
- CVE-2021-34527
- CVE-2019-6111
- CVE-2019-6110



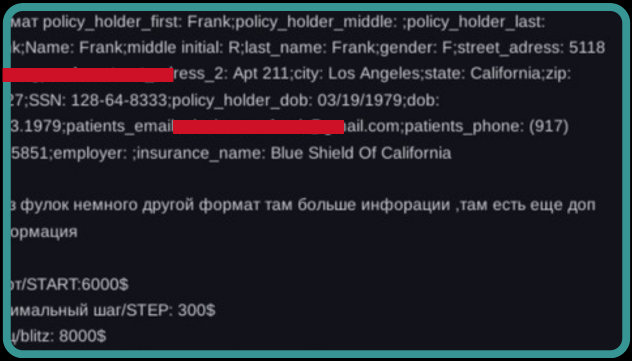
• Top 5 Tools related to actors

In addition, the actors use certain tools to carry out the attacks. Therefore, a list of the most relevant tools ***(from 742 tools used by this kind of actor, registered in xMDR platform)*** in the attacks carried out in the last year has been obtained, which are as follows:

GandCrab ransomware (REvil)
Vatet Loader, Metasploit, Cobalt Strike (RansomHouse)
LockBit ransomware (LockBit)
BlackCat malware (ALPHV)
Munchkin (ALPHV)

The price of data

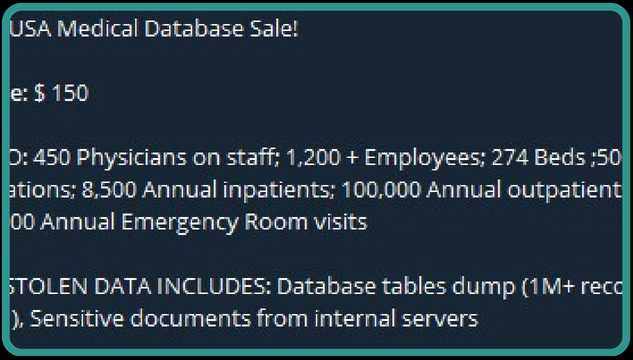
Research carried out by **x63Unit** revealed that the data obtained from ransomware attacks is an asset that provides financial gain in addition to that already obtained from ransomware. A cybercriminal can resell a patient's medical records for between 50-250, as they are among the highest paid for their sensitivity at present.



```
мат policy_holder_first: Frank;policy_holder_middle: ;policy_holder_last:
k;Name: Frank;middle initial: R;last_name: Frank;gender: F;street_adress: 5118
[redacted]ress_2: Apt 211;city: Los Angeles;state: California;zip:
27;SSN: 128-64-8333;policy_holder_dob: 03/19/1979;dob:
3.1979;patients_email[redacted]ail.com;patients_phone: (917)
5851;employer: ;insurance_name: Blue Shield Of California

з фулок немного другой формат там больше инфорации ,там есть еще доп
ормация

от/START:6000$
имальный шаг/STEP: 300$
ц/blitz: 8000$
```

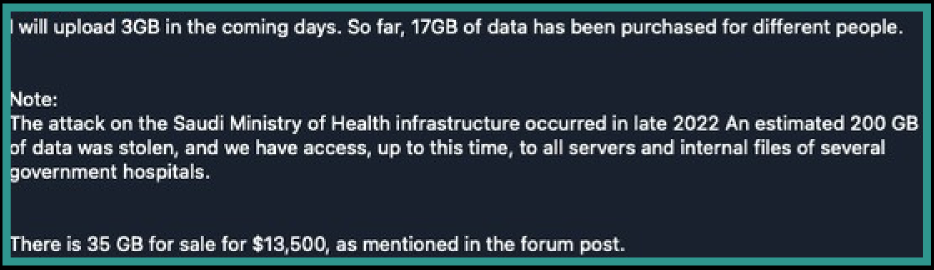


USA Medical Database Sale!

e: $ 150

D: 450 Physicians on staff; 1,200 + Employees; 274 Beds ;50
ations; 8,500 Annual inpatients; 100,000 Annual outpatient
00 Annual Emergency Room visits

STOLEN DATA INCLUDES: Database tables dump (1M+ reco
), Sensitive documents from internal servers

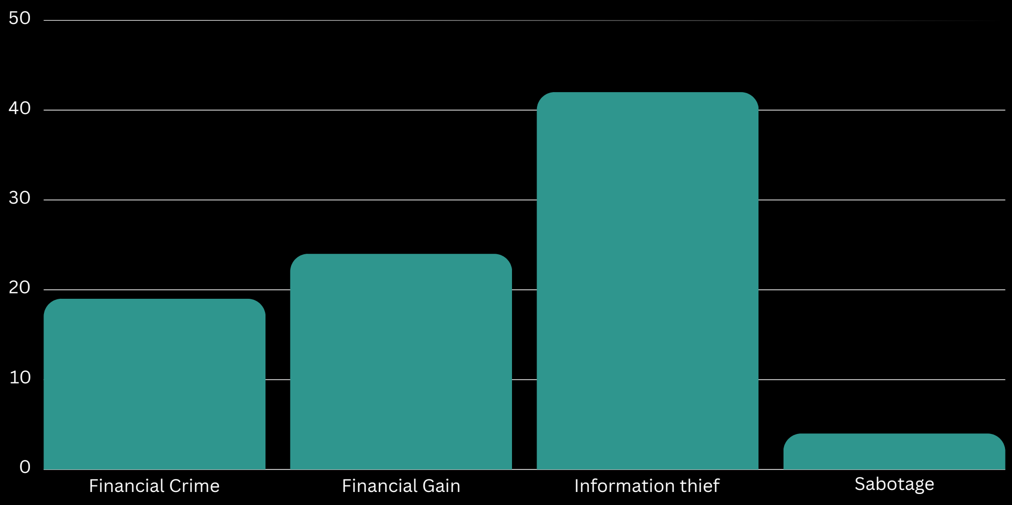


I will upload 3GB in the coming days. So far, 17GB of data has been purchased for different people.

Note:
The attack on the Saudi Ministry of Health infrastructure occurred in late 2022 An estimated 200 GB of data was stolen, and we have access, up to this time, to all servers and internal files of several government hospitals.

There is 35 GB for sale for $13,500, as mentioned in the forum post.

This is why the motivation related to the actors involved in this sector is essentially economic, as information theft is seen as a vector of economic benefit. As it is possible to observe, the value of the sale of this data exceeds the range that is considered usual, as this data is particularly coveted by the cybercrime industry.



Main events in 2023

January

Mindpath Health

Five incidents of unauthorized access/disclosure affecting more than 10,000 individuals.

Febraury

MCNA Dental

700 GB of data stolen from MCNA's systems. Lockbit.

March

Hospital Clínic de Barcelona

Ransomhouse requested a ransom of $4.5 million for about 4.5 TB of information.

April

Robeson Health Care Corporation

Unauthorised access t
confidential data on up o
15,045 patients. t
o

May

DOH Mexico

Leak that affected 49,000 deceased individuals in New Mexico.

June

New Horizons Medical

Attacked by the ransomware group BlackCat. Announcement on its TOR site

July

Medicare and Medicaid Services

1M Medicare beneficiaries suffered a breach due to the massive exploitation of MOVEit

August

Prospect Medical Holdings

RaaS operator stolen 1 TB of documents and 1.3 TB of databases that contained PII information.

September

Johnson Controls International

Encrypted various company devices, including VMware ESXi servers, and 27TB of corporate data was stolen.

October

Postmeds Inc

Data breach affecting 2,364,359 individuals.

November

Ardent Health Services

Ransomware attack in Oklahoma, New Mexico and Texas.

December

Zai Lab

The LockBit ransomware group has claimed responsibility for the attack against the victim.

Ransomware in healthcare Q4

Total Victims (Q4)

14

The king is...

Some data

Top Countries

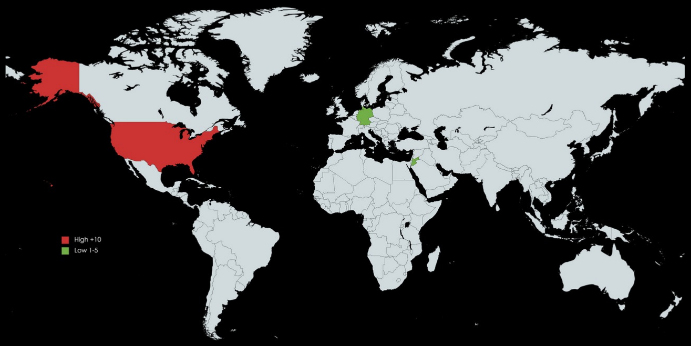
USA - **12**
GER - **1**
JOR- **1**

Sectors

📈inics - **7**
📈ospitals -**3**
📈Associations - **2**
📈harma - **1**
📈 Others - **1**

Top Groups

● Lockbit - **3**
● Everest - **2**
● Cactus - **1**
● BianLian - **1**
● INC - **1**



Victims

- **Ransom victim:** Anna Jaques Hospital - Money Message - Jan 19, 2024
- **Ransom victim:** Northeast Spine and Sports Medicine - BianLian - Jan 14, 2024
- **Ransom victim:** Acutis - Cactus - Jan 12, 2024
- **Ransom victim:** PrimeImaging - Everest - Jan 12, 2024
- **Ransom victim:** Allied - Everest - Jan 12, 2024
- **Ransom victim:** CellNetix - INC - Jan 8, 2024
- **Ransom victim:** Capital Health - LockBit - Jan 7, 2024
- **Ransom victim:** MetroAtlanta Ambulance Service - Cloak - Jan 7, 2024
- **Ransom victim:** Bradford Health - Hunters International - Jan 4, 2024
- **Ransom victim:** Diablo Valley Oncology & Hematology Medical Group - Monti - Jan 4, 2024
- **Ransom victim:** MPM Medical Supply - CiphBit - Jan 1, 2024
- **Ransom victim:** Catholic Hospital Association of East Westphalia - LockBit - Dec 29, 2023
- **Ransom victim:** Abdali Hospital - Rhysida - Dec 26, 2023
- **Ransom victim:** Bay Orthopedic & Rahabilitation Supply - LockBit - Dec 24, 2023

Data from x63Unit

Rules

Detection rules are the culmination of research conducted by the more blue-team oriented segment of the **x63Unit**, focused on **preventing and detecting** malicious behaviors observed in actors, tools, campaigns, or vulnerabilities. This proactive approach is a testament to the unit's commitment to maintaining the highest standards of cybersecurity, constantly evolving to address the dynamic nature of cyber threats.

- **Number of rules: 355**

- **Number of tactics covered from MITRE*: 13 / 14**
- **Number of techniques covered from MITRE*: 120 / 240**

- **ARR* average: 63.016**

🟥	90-100	*Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores*
🟧	70-90	*Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores*
🟨	50-70	*Rules with all or some of these features: Medium attack techniques, risky adversaries (or not related to any), trending (or not) Mitre TTPs, medium CVE scores*
🟢	0-50	*Rules with all or some of these features: Low attack techniques, not related to any adversaries, trending (or not) Mitre TTPs, low CVE scores*

Top MITRE TTP covered:

- Command & Scripting
- System Binary Proxy execution
- User Execution
- OS Credential Dumping
- Impair Defenses

Number of TTPs covered: This value represents the total number of TTPs (Tactics, Techniques, and Procedures) covered by the rules. While achieving 100% coverage is virtually impossible, a coverage rate above 50% is considered exceptionally good.

ARR (Adversary Rule Risk) is an internal score assigned to all rules for representing the risk of the attack technique covered in the rule. In the algorithm score, rule severity, trends, adversary risk and other parameters are used.

Conclusion

The rapid digitalization of the healthcare sector, while beneficial, has undeniably heightened the vulnerability to cyber attacks. The increasing interconnectedness and the vast repositories of sensitive medical data have turned healthcare institutions into prime targets for cybercriminals. The alarming rate of data breaches, compromising the integrity and confidentiality of patient information, has not only financial ramifications but also significantly impacts patient trust and the overall stability of healthcare systems.

The **x63Unit**, with its **specialized multidisciplinary approach** in cyber intelligence, has emerged as a crucial player in this scenario, pushing the boundaries of traditional security measures. By gaining a deep understanding of digital adversaries and their tactics, the unit is adept at developing and implementing comprehensive defense strategies. These strategies are not just reactive but are designed to proactively anticipate and prevent cyber incidents, thus ensuring the highest level of security.

The **xMDR platform**, an innovative solution born from the expertise of the x63Unit, stands as a testament to the unit's ability to translate complex cyber intelligence into effective, client-specific defenses. This platform not only addresses current threats but is also agile enough to adapt to the evolving landscape of cyber threats, offering a level of protection that is unparalleled in the industry.

With the healthcare sector facing its most expensive data breaches in history, and the increasing number of patients affected by these breaches, the importance of robust cybersecurity measures has never been more evident.

Healthcare data available in xMDR Platform

Activities 803

Top 3 Most Relevant

- Lazarus exploiting vulnerabilities
- BreachForums Returns
- North Korea $35M crypto thieft

Counter Operations 74

Top 3 Most Relevant

- Lockbit affiliate arrested in US
- US govt offers bounty for Cl0p
- 11 Indian criminals in prision

Promoted (APTs) 25

Top 3 Most Victim Countries

- APT-28 *(62 Countries)*
- APT-29 (59 Countries)
- DarkHotel (40 Countries)

Threat Adversaries 79

Top 3 Most Victim Countries

- Circus Spider (35 Countries)
- Op.Parliament (27 Countries)
- Carbanak (26 Countries)

Active Groups 18

Top 3 Most Active > 6 Months

- APT-28 (2024-01-12)
- MuddyWater (2023-12-19)
- Lazarus (2023-10-31)

Tools Used 742

Top 3 Most Used By Actors

- Mimikatz *(61 Actors)*
- Cobalt Strike *(58 Actors)*
- LotL *(52 Actors)*

xMDR

powered by Cipher

X63

UNIT

LEGAL NOTICE: NO UNAUTHORISED DISTRIBUTION, USE OR SHARING*****.

This document (hereinafter referred to as "the Document") is the exclusive property of X63 Cipher (hereinafter referred to as "the Owner"). The Owner owns all intellectual property rights associated with the Document, including, but not limited to, copyrights and proprietary rights. Access to this Document is granted only to parties authorised by the Owner for the specific purpose of confidential evaluation.

Any distribution, reproduction, unauthorised use, disclosure or sharing of the Document, in whole or in part, with third parties without the prior express written permission of the Owner is strictly prohibited. Any unauthorised use of the Document shall constitute a violation of the Owner's intellectual property rights and may result in legal action.

Access to and use of this Document are subject to the terms and conditions set forth by the Owner. Any authorised party receiving the Document must comply with the restrictions and obligations set by the Owner. obligations set forth by the Owner. Any questions or requests for permission to distribute, reproduce or use the Document should be directed to the Owner.

Failure to comply with these restrictions may have legal consequences. By accessing or using the Document, you accept and acknowledge the terms of this legal notice.