HEALTHCARE UNDER ATTACK
CYBERCRIMINALS TARGET MEDICAL INSTITUTIONS

BY ANDREW KOMAROV
CHIEF INTELLIGENCE OFFICER INFOARMOR, INC.
HEALTHCARE UNDER ATTACK
CYBERCRIMINALS TARGET MEDICAL INSTITUTIONS

InfoArmor has identified a group of bad actors performing targeted cyberattacks on healthcare institutions and their IT infrastructure, including connected medical devices such as Magnetic Resonance Imaging systems (MRI), X-ray machines and mobile computing healthcare workstations.

This group of bad actors has performed at least four successful attacks against US-based organizations of varying size, compromising a significant number of medical records. The threat actors claim to have stolen millions of medical records and gained unauthorized access for ransomware distribution.

In mid-May 2016, InfoArmor notified the National Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC), along with the appropriate parties concerning the incident, providing them with relevant information for further investigation and identification of the key bad actors.

According to InfoArmor’s Chief Intelligence Officer Andrew Komarov, such healthcare information systems are targeted based on the sensitive data that they contain. Successful attacks allow bad actors to penetrate deep into the network environment and exfiltrate this sensitive data on a wide scale basis. These breach incidents expose sensitive patient data and create significant HIPAA healthcare privacy exposures that require substantial response and attention.
One of the key targets of the intrusion identified in this campaign was the Electronic Health Records (EHR) Software System.

Fig. 2 – The bad actors received access to the EHR system on the compromised host on SRS EHR v8 by SRSsoft, a widely used centralized medical records management system.
These systems contain detailed information about patients including their personal health information (PHI), medical history, diagnoses and internal information used by the healthcare institution.

Fig. 3 – The compromised EHR system disclosed sensitive information including SSN number, medical history, diagnoses and additional details that breached patient privacy.
In some cases, these systems stored all of the data in local files or in the Microsoft Access desktop databases without any special user access segregation, which created a serious risk of data theft once the network host was compromised.

Fig. 4 - Example of thousands of compromised medical records related to patients of the affected healthcare institution in the State of Montana
HEALTHCARE UNDER ATTACK
CYBERCRIMINALS TARGET MEDICAL INSTITUTIONS

Fig. 5 - Compromised EHR System - bad actors have access to patient specific biometrics, PHI, medical records or other sensitive data.
Cybercriminals tried to sell over 3 terabytes of stolen data from healthcare institutions including SSN numbers and detailed patient information on differing underground communities.

<table>
<thead>
<tr>
<th>RDP Access to another Healthcare Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceMon - (C++ Key/Screen/Clipboard Monitor) [XP - W10] - 110 kb ~ swayz</td>
</tr>
<tr>
<td>RDP access to an American hospital's NETWORK (~3TB data: SSN, DOB and much more)</td>
</tr>
<tr>
<td>Insurance Provider Logins</td>
</tr>
<tr>
<td>arnie</td>
</tr>
<tr>
<td>[SELLING] Fullz (SSN, DOB, NAME, ADDRESS, +++</td>
</tr>
<tr>
<td>f3ttywap</td>
</tr>
<tr>
<td>[SELLING] Banking Bot [Rootkit] [FASM]</td>
</tr>
<tr>
<td>supernickjob</td>
</tr>
</tbody>
</table>

Fig. 6 - The identified group was targeting US healthcare institutions specifically and stealing large numbers of medical records for further identity theft and ransomware distribution.
CONCLUSION

InfoArmor warns healthcare institutions that use smart medical devices and computerized electronic health records systems (EHR) about the growing interest in targeted attacks from cybercriminals. Network system infiltration may expose healthcare organizations to a variety of negative impacts including data exfiltration compromising and exposing the PHI of its patient population, medical identity fraud, and/or extortion through ransomware which, in a worst case scenario, could lead to loss of life.

In order to react proactively to the growing probability that these intrusions will occur, InfoArmor highly recommends that healthcare institutions subscribe to additional security services for personal data and privacy protection, including InfoArmor’s enterprise based Advanced Threat Intelligence services along with employee behavior training and personnel protections included with PrivacyArmor Secure.

ABOUT INFOARMOR

InfoArmor offers industry-leading identity and cyber intelligence services that help our clients fight emerging fraud and advanced cyber threats. We combine an unparalleled global research network with big data analysis, actionable intelligence and customized service to meet clients’ dynamic security needs. From employee to enterprise, InfoArmor is redefining how organizations fight fraud and combat an evolving threat landscape to mitigate risk on multiple levels. Today, more than 600 businesses and government agencies, including 50 of the Fortune 500, use PrivacyArmor®, the industry leading employee identity protection solution, or VigilanteATI®, our award-winning advanced threat intelligence platform to improve their data security posture.

For more information please visit the InfoArmor website at infoarmor.com, or contact InfoArmor sales at +1 480 302 6701, or email sales at ati@infoarmor.com.