Recorded Future | Support

Recorded Future: Support › Insikt Group › Threat Research Blog

Search

Access to Two Medical Practices Offered for Sale

Insikt Group 8 days ago

By Andrei Barysevich

Key Judgments

- A previously unknown Russian-speaking hacker is offering access to two medical offices in New York and Michigan, which includes access to records of 15,000 New York patients and 11,000 in Michigan.
- Both medical offices utilize eClinicalWorks software; however, miscreant claims access was obtained via compromised VNC protocol.
- Ruben U. Carvajal, MD was identified as the actor's New York victim.
- The second victim was identified as Adham-Sayed-Ali, MD, operating out of East Dearborn Medical Center.
- According to the seller, as of this writing no patient records from compromised systems were retrieved.
- Recorded Future alerted federal law enforcement of both incidents.

Background

On December 19, 2017, ek0t (Intel Card), a newly registered member of the popular hacking forum Exploit offered for sale access to the internal computers of two medical offices in New York and Michigan. According to the actor, the buyer will be able to access approximately 15,000 New York patients and 11,000 records for the compromised Michigan office.

Insikt team was able to establish contact with the seller and confirmed ek0t's claims, obtaining enough evidence to conclude that the New York system belongs to Ruben U. Carvajal, MD, operating out of two locations in Bronx, while the second Michigan victim remains unknown.

According to the screenshots provided by the seller, both medical practices are using eClinicalWorks software, a popular choice among many medical institutions nationwide, and both networks were accessed via compromised Virtual Network Computing (VNC), often used legitimately to access and control computer systems remotely.

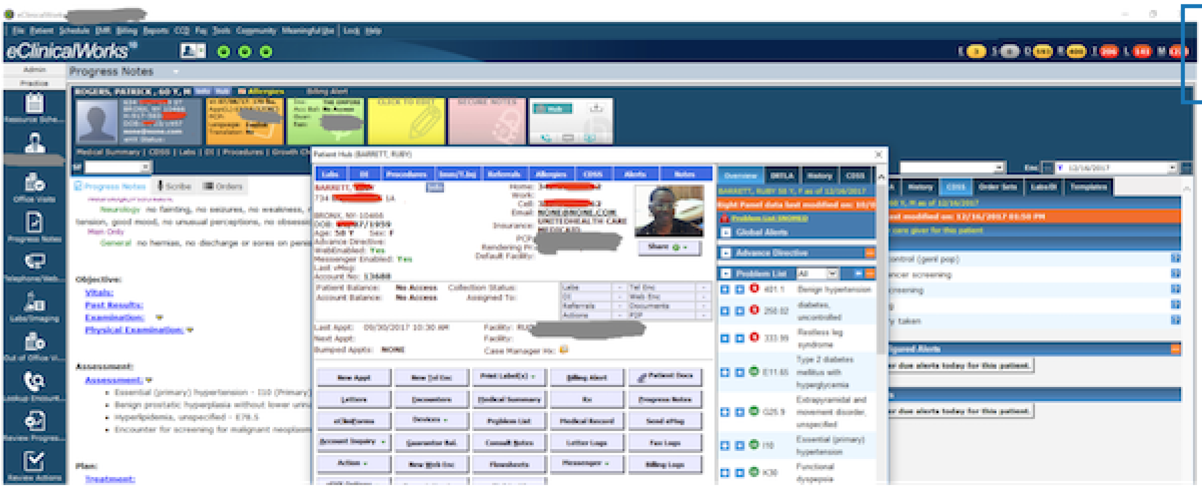
At the time of this writing, ek0t has confirmed that no patient records were retrieved from compromised systems.

Updated January 4, 2018

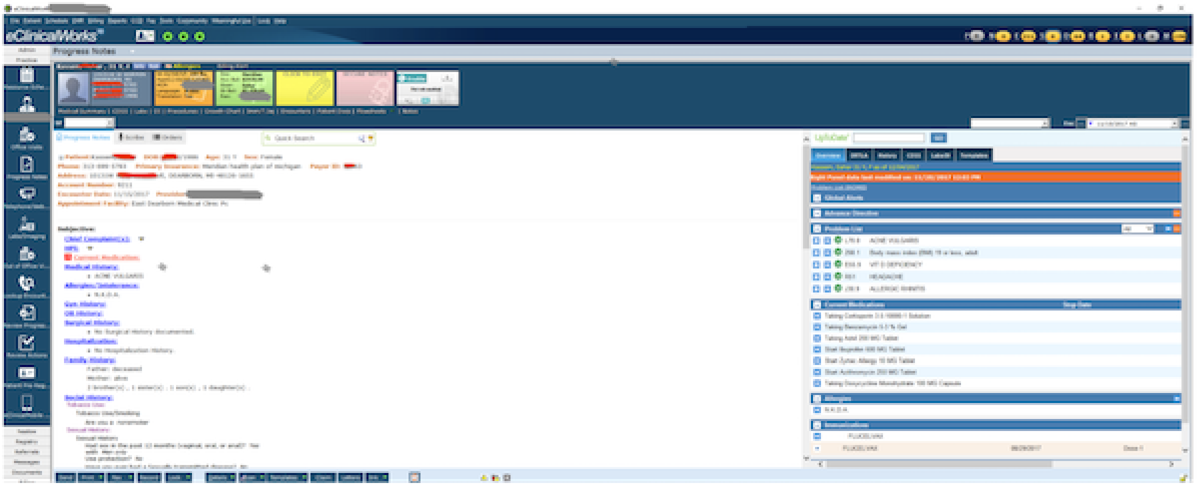
On January 4, 2018, Insikt group was able to confirm with a high degree of certainty the identity of the second victim. Adham-Sayed-Ali, MD operating out of East Dearborn Medical Center in Dearborn, Michigan.

According to the seller, victim’ servers have been inaccessible since December 28; the miscreant never downloaded 2017, likely due to the holiday schedule and no patient's data. Recorded Future continues assisting law enforcement in their investigation of both breaches and will update the report accordingly.

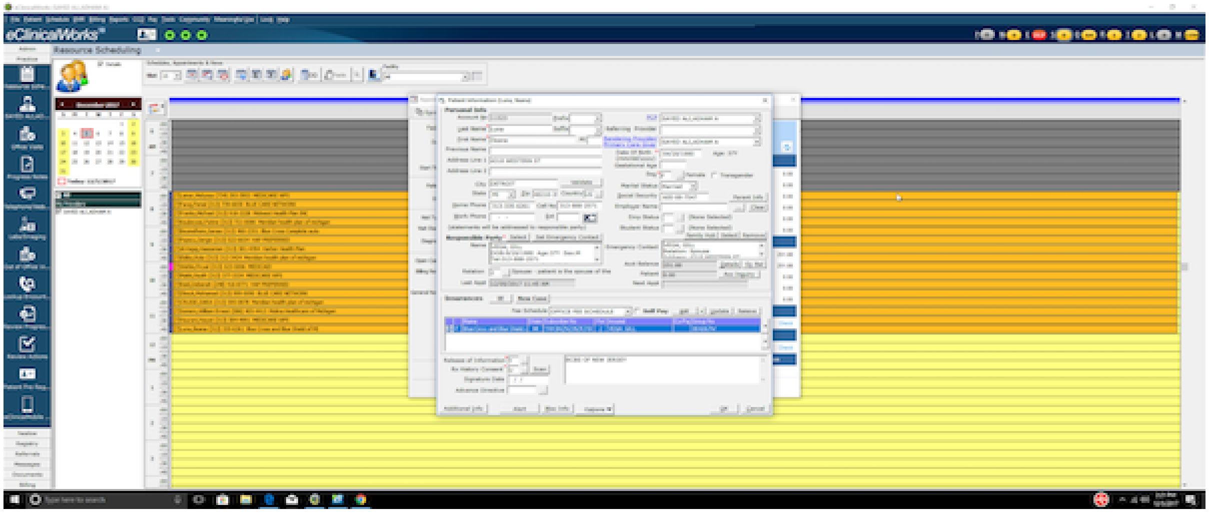
Appendix A: Screenshots



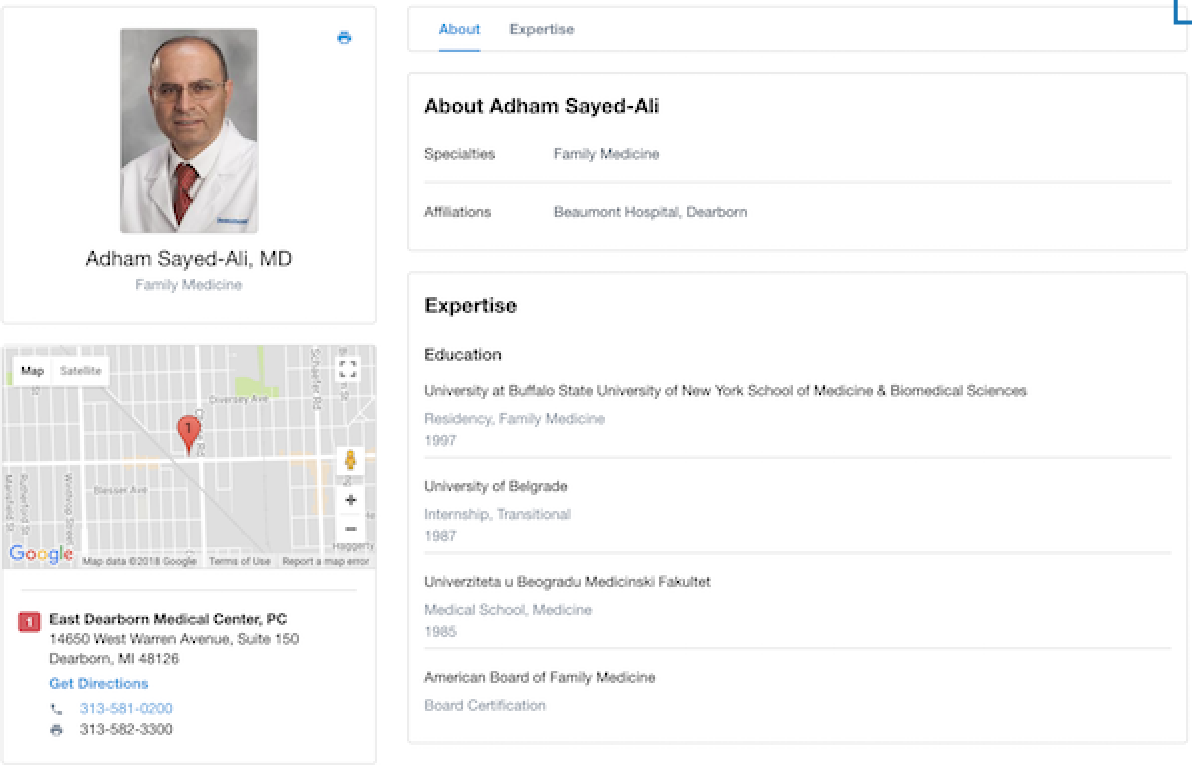
Screenshot of New York patient record provided by the hacker.



Screenshot of Michigan patient record provided by the hacker.



Screenshot of Michigan patient record provided by the hacker, revealing the name of the victim.



About Expertise

Adham Sayed-Ali, MD

Family Medicine

About Adham Sayed-Ali

Specialties	Family Medicine
Affiliations	Beaumont Hospital, Dearborn

Expertise

Education

University at Buffalo State University of New York School of Medicine & Biomedical Sciences
Residency, Family Medicine
1997

University of Belgrade
Internship, Transitional
1987

Univerziteta u Beogradu Medicinski Fakultet
Medical School, Medicine
1985

American Board of Family Medicine
Board Certification

1 East Dearborn Medical Center, PC
14650 West Warren Avenue, Suite 150
Dearborn, MI 48126
Get Directions
☎ 313-581-0200
313-582-3300

Adham-Sayed-Ali, MD servers were compromised by ek0t.

Was this article helpful? 👍 👎

1 out of 1 found this helpful

The content of this article is confidential and intended solely for the use of individuals with authorized access to the Recorded Future service. Do not download or distribute this article.

Have more questions? Submit a request

Comments

3 comments

Sort by ⌄

David Marcus January 02, 2018 06:39

0

I found this VERY useful. Medical record compromise is of prime interest to my group.

Matthew Hodyno January 03, 2018 07:26

0

Excellent work!

Omar Duran January 15, 2018 10:37

0

Nice job!!! If you have something similar for the Energy Sector please share.

Please note that your name will be displayed.

SUBMIT

Related articles

Vendors Rush to Patch Meltdown and Spectre Vulnerabilities

Actor Profile: IZG0Y

North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign

Threat Leads Roundup – Week of 12/25/17

Threat Leads Roundup – Week of 01/08/18