Nokod Security

Re: Support letter for best project competition – Anna Novin and Barak Sofir: Resilient C&C Communication Based on Public Infrastructure

My name is Amichai Shulman. I am currently the co-founder and CTO of Nokod Security, I was co-founder and CTO of Imperva for 15 years, and co-founder and CTO of AirEye. I serve on the advisory board of multiple cyber security companies. I am also an adjunct teacher in the Technion. I supervised the work of Anna Novin and Barak Sofir on the project of “Resilient C&C communication based on public infrastructure” as part of the course “Project in Information Security” (236349) under the academic supervision of Prof. Eli Biham. The project was submitted for the Winter 2022/2023 Semester.

C&C infrastructure is a critical component of any modern cyber attack campaign, hence researchers and incident response professionals developed techniques and tools to dismantle these as soon as an attack is detected - in a way that cannot be reconstructed. That is, all the effort invested in infecting machines with bots goes down the drain. Only well funded nation state adversaries were able to create C&C infrastructure that are stealthy and resilient enough over time. The goal of the project was to prove that creating a super resilient C&C infrastructure can be achieved in cost effective ways that would enable even low end attackers to survive a takedown when detected. A successful implementation of this concept should drive the cyber industry into developing new methods and technologies to cope with this new threat.

Anna and Barak tackled the problem from start to end. They evaluated several public cloud services in order to find a suitable basis for their system (Reddit) to serve as the basis for their system, they designed a communication system to run on top of that platform in a manner that is extremely difficult to detect and more importantly, one that is impossible to dismantle. Finally, they were able to revise their system in a manner that allowed full-duplex communication between the bots and the controller.

Barak and Anna designed their system in a manner that does not require the controller of the botnet to create new content in the Reddit platform but piggyback on other people’s content. By carefully choosing the content to piggyback on they were able to avoid any chance of detection by prying eyes, literally hiding the control messages in plain sight. They used search functionality in the Reddit platform to initialize communication between the bots and the bot controller which is the key to making the botnet impossible to dismantle. Last, but not least, they discovered that under some circumstances accounts in the platform can be opened and maintained with no access to a real email address and used that in order to establish a reverse communication channel from the bot to the controller (again, through comments on Reddit content).

Throughout the work on the project Anna and Barak demonstrated independence, creativity, high technical skills, and perseverance. They were able to build a fully functional proof-of-concept for a novel cyber attack concept by combining multiple tactics and techniques. For their work on this project, I recommend that they receive the best project award for this year.

Amichai Shulman
CTO
amichai@nokodsecurity.com
https://www.linkedin.com/in/amichaishulman/

Audit Trail

Signeasy

This audit trail was created during the document signature process and holds details of parties involved, including email address of signer(s), device IPs, signature timestamp and more. It serves as a digital certificate and can be used as a legal evidence.

FILE NAME	AnnaNovin-ProjectRecommendation.pdf
DOCUMENT REFERENCE ID	99b98e06b0e24e96a2003fbb8355aa60
TIME STAMP	24 May 2023 20:48:21 UTC
DOCUMENT FINGERPRINT	5417e754888a4ffe5ec11f762bd1ccddda7c94cb1c08163cf374e38befa4e3ca
IP ADDRESS	79.181.71.101
USER REFERENCE ID	243794e7e6ac48698c941b30eaa4c17e
EMAIL ADDRESS	amichai.shulman@gmail.com
VERIFICATION LINK	https://app.signeasy.com/verify/wnVKEPqd9SWAbBQS_47_8g==/

LEGAL
Electronic signature are legally binding and admissible in a court of law in accordance with the ESIGN Act in United States and eIDAS in the European Union. Most of the other countries around the world as well have adopted an electronic signature law or have recognized electronic signatures for business or personal transactions.

SECURE
This document was securely processed using 256 bit SSL encryption technology for the communication channels between your device and the secure servers hosted at Amazon Web Services, which is ISO 27001 compliant.

TRUST
Signeasy is trusted and used by thousands of companies and millions of people in over 150 countries.

Learn more at https://signeasy.com