# OpSec provided Bayrob Group a decade of crime.

David L. Fulton[1]*

**Issue**

Bayrob Group's arrest and prosecution provides a window into a cybercrime group that had fantastic operational security for nearly a decade of operation.

[1] *Department of Computer Science and Engineering, Bagley College of Engineering, Mississippi State University*

## Background

In the mid 2000s a small time cybercrime group that became known as the Bayrob Group started operating out of Romania. The group was named by Symantec based on its early crimes involving eBay.com.[1] What makes this group interesting is its size, operational capacity, and operational security. During their near decade long run they managed to steal between four and thirty five million dollars from primarily American targets. The thefts ranged from sales scams to credit card fraud and cryptojacking.

**The small size** of the Bayrob showcases the concentrated power small teams can have. The group consisted of Bogdan Nicolescu, Radu Miclaus, and Tiberiu Danet. Mr. Nicolescu was the group leader and provided the strategic direction of the groups growth and development. Mr. Tiberiu was their lead malware developer and botnet author. Interestingly Mr. Tiberiu's skill was such that in 2008 while still a student, was elected to be on Romania's National Computer Science Team.[1] Mr. Miclaus is described as being the group's manager for auction fruad[1] and a "junior technical member"[2].

**The operational scope** of this team developed over time. Initially it used used auctions for vehicles as a means to source victims. The group would run an auction to find interested parties. Then they would cancel the auctions and later contact the victims with a story that the sale had fallen through, along with pictures that included personalized malware for the victim. They would offer the vehicle at a slightly reduced price and if the victim attempted to buy the car, the malware would inject false web pages and redirect the victim to a false site to complete the transaction. This personalized and directed criminal work kept them as small time operators.

In time Mr. Nicolescu would lead them into other operations. The malware would progress from simple and personalized attackware to impersonal keyloggers and bank fraud to pay for the infrastructure as well as theft and money transfers.

The rise of bitcoin saw them move from targeted attacks to massive infrastructure based cyber-

[1] BotHurder and lead funds propagation agent.

crime. They developed a botnet[2] estimated to have included 300,000 - 400,000 machines to provide Bayrob the infrastructure to run crypto coin mining operations. Such illicit use of computers computing power is termed ”CryptoJacking”.

**Their operational security** was key to their success and long term operational success. They used stolen credit cards gained from their keyloggers to purchase websites. These websites where algorithmically determined and where the first of a multilayered of command and control(CnC) system. Each step would reduce operational risks.[3] The group also used encrypted emails, encrypted messaging, and multiple layers of VPNs to mask their identities.

## Current Status

Ultimately the group was captured due to two failures. First, there was an ”error” [1] in the VPN software that opened up their operations to a degree without revealing who the people running the botnet were. Second, Mr. Miclaus forgot to logout of the VPN and accessed their real AOL account rather than the spam sending AOL account[3]. The simple act of checking their email from their ”secure” VPN was the break in operational security the FBI needed to get a silent search warrant.

Mr. Danet happened to visit Miami, unaware that there was a warrant to search is possessions on entry to the country. Based on the contents of his phone, the FBI was able to issue an international arrest warrant and the Romanian Police apprehended and extradited the trio.

## Key Considerations

The court filing of these men provide a clear and detailed account of a cybercriminals' methods and operations. [4] The document provides a clear explanation of how cyber crime can operate and the methods to evade arrest.

The work of Bayrob Group is notable in the depth of operational security maintained for such a long time. The clever use of malware that could only connect to the first step in a chain of connections provided deniability and the use of multiple VPNs and encryption provided the secrecy and deniability that allowed for a very long run.

It should be noted that a team of 3 managed to steal $4 - $35 million over 10 years. The size of the cybercrime group is amazing and scary. The largest issue they seemed to face was exfiltrating the money stolen and they used a series of curriers to move the cash or object bought and later sold for cash. This appears to be the hurdle to cybercrime, how to cash out the thefts.

## Conclusion

The Bayrob group's capture[2] and prosecution [4] provides cyber security students a look into the oper-

[2] PreInternet Of Things
[3] Browser auto-fill for the ”win”?

ations of a cybercrime group that was very successful and amazingly opeationaly secure. This should be viewed along side the work by Christopher Bing and Joel Schectman showcasing the UAE's Project Raven[5], a work that explains how nation-state operations are handled and the Secretary of the Navy's Cybersecurity Readiness Review[6]. Combined, they provide an understanding of the scope and motivations of the threat actors in cyberspace.

## References


[1] Catlin Cimpanu. The bayrob malware gang's rise and fall - the story of how a talented computer science student and his friends created and ran a multi-million dollar botnet. *New York Times*, 13 Apr 2019. Viewed: 21 Apr 2019 https://www.zdnet.com/article/the-bayrob-malware-gangs-rise-and-fall/.

[2] Symantech Security Responce. Bayrob: Three suspects extradited to face charges in us. Blog, Symantec, 16 Dec 2016. Viewed: 21 Apr 2019 https://www.symantec.com/connect/blogs/bayrob-three-suspects-extradited-face-charges-us.

[3] Matthew Monte. *Network Attacks and Exploitation a Framework*. Wiley, 2015.

[4] Patricia Anne Gaughan. United states v. nicolescu (1:16-cr-00224) district court, n.d. ohio. *Court Listener*, 18 Apr 2019. Viewed: 21 Apr 2019 https://www.courtlistener.com/docket/4555763/united-states-v-nicolescu/.

[5] Christopher Bing and Joel Schectman. Inside the uae's secret hacking team of american mercenaries ex-nsa operatives reveal how they helped spy on targets for the arab monarchy — dissidents, rival leaders and journalists. *Reuters*, 30 Jan 2019. Viewed: 30 Jan 2019 https://www.reuters.com/investigates/special-report/usa-spying-raven/.

[6] Secretary of the navy cybersecurity readiness review. *Navy*, Mar 2019. Viewed: 24 Mar 2019 https://www.navy.mil/strategic/CyberSecurityReview.pdf.


## About the Author


**David L. Fulton** is pursuing a MS Cybersecurity and Operations degree with an operations concentration. He has a BSc. Computer Engineering from UC Santa Cruz, an MBA and a MS in Information Systems from Mississippi State University (MSU).

He is a Senior Web Developer for Enterprise Information Systems at MSU and taught Software Architecture for the Department of Computer Science and Engineering at MSU


**Department of Computer Science and Engineering** Recognized nationally for its leadership in cyber security, MSU is one of only nine schools to hold all three of the National Security Agency's centers of academic excellence credentials:

- CAE-Cyber Defense Education
- CAE-Cyber Defense Research
- CAE-Cyber Operations

**Bagley College of Engineering** It currently ranks 51st among all engineering colleges nationally in research and development expenditures according to the National Science Foundation. U.S. News and World Report ranks its undergraduate and graduate programs in the top 100 nationwide.