CrimeOps: The Operational Art of Cyber Crime

sec.okta.com/articles/2020/08/crimeops-operational-art-cyber-crime

‹ Back to blog
August 4, 2020
The Grugq

Cyber Crime Innovation Is Lucrative

Cybercrime rewards innovative organizations. These can innovate at the tactical level (e.g. new or updated tactics, techniques, and procedures (TTP)), the strategic level (e.g. new monetisation methods), or at the operational level—the management of resources and personnel to achieve strategic objectives. This is operational art.

The operational level, the glue that enables a group to execute well, is seldom analyzed because it is rarely visible to information security researchers. Unlike tactical TTP, where changes are discovered quickly on the ground, new operational strategies only come to light by monitoring major shifts and trends.

The FIN7 affidavits are a unique opportunity to see inside the management of a successful cybercrime gang and analyze their operational art. The most detailed information in the affidavits covers the time period 2016–2017. The methodologies and tooling described were cutting-edge and trendy at the time

The Innovators—FIN7, Uber for Cybercrime

Kaspersky has been tracking FIN7 since 2015 . Despite a series of arrests in 2018–2020, and ongoing investigations, FIN7 continues to operate. FIN7 managed hundreds of victims, huge volumes of stolen data, a large salaried team, development of new targets, and maintaining their tool chain. That’s an organisation with a lot of moving parts. Their innovations were in cyber crime operational art. The details of how this group of Russian cyber criminals cooperated as an organisation is fascinating.

FIN7 was not and is not the most technically sophisticated threat actor. They rely on phishing for access, their toolkit is just repurposed common malware, and they monetize via stolen credit cards and wire transfers. Despite being only a middle of the road hacking outfit, they looted an alleged 1 billion US dollars by 2018. Why was FIN7 so amazingly successful using only stodgy *“Top 10 Infosec Risks”* TTP?

The answer is FIN7’s sophisticated organisation and management capabilities. They adopted agile processes and a DevOps methodology. Good team coordination and project management tools were combined with rapid iteration on their toolchain and TTP to maintain efficacy and operational capability. Let's explore CrimeOps.

CrimeOps: Project Management for Criminals

The secret of FIN7’s success is their **operational art of cyber crime.** They managed their resources and operations effectively, allowing them to successfully attack and exploit hundreds of victim organizations. FIN7 was not the most elite hacker group, but they developed a number of fascinating innovations. Looking at the process triangle (people, process, technology), their technology wasn’t sophisticated, but their people management and business processes were.

Their business… is crime! And every business needs business goals, so I wrote a mock FIN7 mission statement:

> *Our mission is to proactively leverage existing long-term, high-impact growth strategies so that we may deliver the kind of results on the bottom line that our investors expect and deserve.*

How does FIN7 actualize this vision? This is CrimeOps:

- Repeatable business process
- CrimeBosses manage workers, projects, data and money.
- CrimeBosses don’t manage technical innovation. They use incremental improvement to TTP to remain effective, but no more
- Frontline workers don’t need to innovate (because the process is repeatable)

Let’s look at their process triangle.

People: FIN7 Team Roles

The organization had a surprisingly sophisticated range of job functions and an impressive depth of capability, similar to that you'd need to build an APT.

- Managers
- Operators
- Developers
- Interpreters

The FIN7 group grew capacity by hiring people via fake front companies. Behind the facade of their fake information security company, the leaders of FIN7 recruited employees to work on development and penetration testing. Prospective employees were interviewed on a HipChat instance (a sort of privately hosted Slack).

> *"By 2025 there will be a projected shortage of 20,000 cybercriminals"*
> *– Cyber Crime Business Weekly, probably.*

FIN7 is currently suffering a number of setbacks as the FBI aggressively dismantles it. The executive suite is being cleared out. Leaders of the group (the management team) have been arrested, but a large number of supporting players have escaped the long arm of the law.

Process: How to Cyber Crime and Make Money

FIN7's success comes from their effective crime process, a monetization template that easily adapts to different verticals and organisations. The fundamental cyber crime process used by FIN7 is unremarkable, but absolutely effective. It's bread and butter cybercrime. The process that converts access to a company into a stream of valuable financial data and money transfers is:

1. Select target
2. Research potential assets in target
3. Recruit asset over email
4. Trick asset into deploying remote access Trojan
5. Survey network
6. Start continuous exfiltration
    1. Access business bank accounts, access point of sale or other financial processing
    2. Transfer money out of accounts, transfer collected data out of network
7. Sell financial data

This is a black box that makes money. A target, as input, produces wire transfers and financial data as output. The innovation was in scaling this process.

A reliable crime process enables value extraction from any victim. Therefore the business strategy for this criminal enterprise is not value extraction, but growing the portfolio of victims they can exploit. Essentially, once they had product/market fit, FIN7 just had to scale. The scaling bottleneck is not in the process, but in executing it in parallel. This is where the operational art of cyber crime becomes portfolio management.

Business Growth: Portfolio Management for Hackers

> *"Portfolio management is the selection, prioritisation and control of an organisation's programmes and projects, in line with its strategic objectives and capacity to deliver. The goal is to balance the implementation of change initiatives and the maintenance of business-as-usual, while optimising return on investment."* – APM Body of Knowledge 7th edition

After the core team standardized their process for exploiting a victim company, the bottleneck to maximising returns moved from “develop a process” to “run the process in parallel.” FIN7’s innovation in operations, project, and resource management allowed them to grow their actively exploited victim portfolio.

This is portfolio management. The portfolio is a bundle of projects. Each project is a victim company moving through the monetization process with associated resources. A project contains information about the victim, assigned personnel, and extracted data. The only way to handle hundreds of victims is with a project management software stack to track and monitor the progress through the process.

FIN7 also used the project management processes of its time, including agile and DevOps. They used agile (iterative changes in response to feedback) to adjust and change their tooling as necessary to remain operational. They used DevOps as collaboration between developers and operations with central management throughout the end-to-end engineering process.

Technology

Tactically FIN7 is boring. The tactical cybercrime process, the TTP which enables the process, is fairly rigid. FIN7 have been tracked by their TTP, and other groups have been found duplicating the TTP (can you get a patent for a cyber crime business process?), for years. There is not much room to innovate at the tactical level, and it is unlikely that innovation would substantially alter their revenue because they are not bottlenecked by their ability to penetrate or extract value. With boring but effective tactical technology, frontline workers don’t have to innovate, and revenue is not dependent on their technical skills.

Success is realized through innovative management. FIN7 used project management software to track victims and the progress of their attacks. They used group chat software to manage personnel, conduct interviews, and trade data. A separate secure chat system was used for sensitive operations, such as arranging salary payment.

Using JIRA, FIN7 created an issue ticket for each victim. As the attack progressed through reconnaissance, infiltration, lateral traversal, and target exploitation (by collecting data into "loot"), the issue was updated. Usernames and passwords, output from security tools, screenshots and video captures, everything relevant to increasing their access and control over the victim, was added to JIRA.

It is interesting that JIRA was used as an information management tool, with a single issue per victim and relevant information added as comments. This is a poor use of JIRA's capabilities. They did not use JIRA’s project management functionality, but instead abused ticketing for ad hoc collaboration. This could be improved—information management would be handled better with a wiki or a specialized red team collaboration tool.

It is possible that JIRA was used partially to help maintain the cover of the "legitimate" Combi Security company. Realistically, any penetration tester who was involved in FIN7's criminal operations would know that they were not conducting ethical hacking, because:

- Proper pen tests have start times, kickoffs, and duration
- Pen test customers supply information to the pen test team
- Sophisticated social engineering is seldom used (because it always works)

There were overtly criminal indicators:

- Targeted social engineering with tailored enticements and infection vectors
- Secondary social engineering pressure (phone calls to guide victim through the infection process)
- Using malware for post exploitation
- Targeting point of sale systems
- Collecting credit card details in "loot.rar"

Really though, the number one reason is more obvious—**pen tests always result in report writing**.

CrimeOps: Continuous Infiltration Pipeline

We have reviewed FIN7's CrimeOps process triangle. Key innovations and improvements to standard practice developed or adopted by FIN7 were:

- Move from technological innovation to business innovation
- Repeatable adaptable process
- Portfolio management to scale the processes
- Project management software to track large numbers of victims
- Capacity building to execute processes in parallel
- Team roles, structured teams, and recruitment
- DevOps collaboration
- Agile rapid iteration on toolkit

Crime pays when you move up the value chain into project management!

The Grugq is a pioneering information security researcher with two decades of experience at almost every level of the field. He has worked extensively with threat intelligence, disinformation, digital forensic analysis, binary reverse engineering, rootkits, mobile phone security, Voice over IP, telecommunications and financial services security. The Grugq has been quoted and referenced routinely in The New York Times, Washington Post, Forbes, Wired, TechCrunch, BoingBoing, VICE and BBC News. Grugq's quotes and insights are so frequently referenced at security conferences that he's informally known as the "most quoted man in infosec".