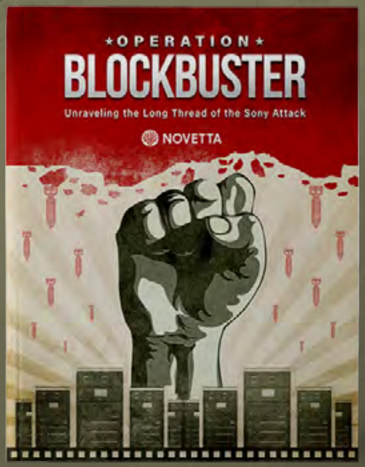
EXECUTIVE SUMMARY

NOVETTA



DOWNLOAD THE FULL OPERATION BLOCKBUSTER REPORT AT:

www.OperationBlockbuster.com

OPERATION BLOCKBUSTER

Unraveling the Long Thread of the Sony Pictures Attack

INTRODUCTION

The 2014 Sony Pictures hack was one of the most shocking and significant cyber attacks against a U.S. commercial enterprise to date. The incident caused significant financial and reputational damage to Sony Pictures and its executives. Most importantly, it illustrated how little resistance a corporate enterprise is able to provide in the face of a capable and determined adversary with destructive intent.

In Operation Blockbuster, a Novetta-led coalition, comprised of the Novetta Threat Research & Interdiction Group (NTRIG) and private industry partners, identified and interdicted the adversary behind the Sony Pictures attack. The coalition links this adversary – dubbed “the Lazarus Group” – to the repeated use of particular malware code and numerous malicious attacks against commercial, military and government targets, dating as far back as 2009.

KEY TAKEAWAYS

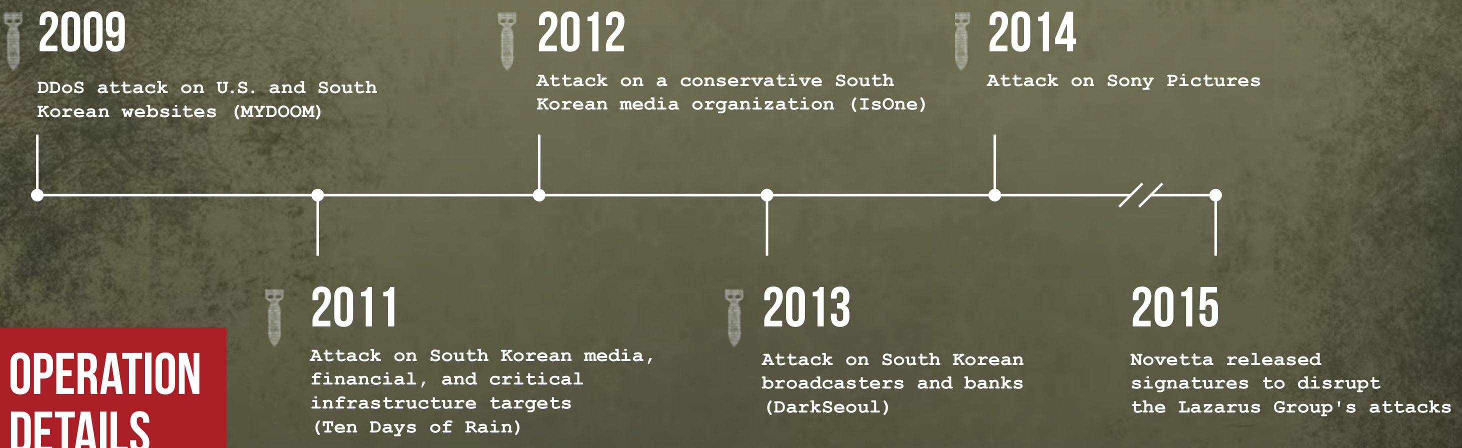
- Malware used in the November 2014 Sony Pictures attack is definitively linked to malware developed as early as 2009.
- The same malware has been used to target government, media, military, aerospace, financial, and critical infrastructure entities, primarily in South Korea and the United States.
- The depth and scope of evidence suggests that the Sony Pictures attack was carried out by a well-structured, well-resourced and highly motivated organization, and not the work of a pop-up hacktivist group.
- Novetta’s coordinated, ongoing response illustrates that in this new era of cyber defense, private industry’s role has changed from “observe and report” to “observe and act.”

MALWARE FAMILIES

THE LAZARUS GROUP

DELTA	DDoS	DeltaAlfa DeltaBravo DeltaCharlie
HOTEL	HTTP Server	HotelAlfa
INDIA	Installer	IndiaAlpha IndiaBravo IndiaCharlie IndiaDelta IndiaEcho IndiaFoxtrot IndiaGolf IndiaHotel IndiaIndia IndiaJuliett IndiaKilo IndiaWhiskey
KILO	Keylogger	KiloAlfa
LIMA	Loader	LimaAlfa LimaBravo LimaCharlie LimaDelta
PAPA	Proxy	PapaAlfa
ROMEO	RAT	RomeoAlfa RomeoBravo RomeoCharlie RomeoDelta RomeoEcho RomeoFoxtrot RomeoGolf RomeoHotel RomeoMike RomeoNovember RomeoWhiskey
SIERRA	Spreader	SierraAlfa SierraBravo SierraCharlie SierraJuliett-MikeOne SierraJuliett-MikeTwo
TANGO	Tool (Non-classed)	TangoAlfa TangoBravo TangoCharlie TangoDelta
UNIFORM	Uninstaller	UniformAlfa UniformJuliett
WHISKEY	Destructive Malware (“Wiper”)	WhiskeyAlfa WhiskeyBravo WhiskeyCharlie WhiskeyDelta

MOST WIDELY REPORTED LINKS TO LAZARUS GROUP


2009
DDoS attack on U.S. and South Korean websites (MYDOOM)

2011
Attack on South Korean media, financial, and critical infrastructure targets (Ten Days of Rain)

2012
Attack on a conservative South Korean media organization (IsOne)

2013
Attack on South Korean broadcasters and banks (DarkSeoul)

2014
Attack on Sony Pictures

2015
Novetta released signatures to disrupt the Lazarus Group's attacks

OPERATION DETAILS

In the weeks following the Sony Pictures hack, US-CERT released an alert detailing a set of malware families used by unidentified attackers to compromise large network infrastructures and deploy hard-drive wiping malware, RATs, and proxy trojans.

Novetta's analysis of the base set of malware revealed that common code libraries were used across multiple malware families. The Operation Blockbuster team used these libraries to generate signatures to detect additional malware samples, including more than 45 distinct malware families that fall under the Lazarus Group's domain.

Novetta, with the help of operation partners, made available signatures that identified Lazarus Group tools on a broad scale, effectively disrupting the group's ability to use these tools for malicious intent.

ACRONYM KEY:

US-CERT:
United States Computer Emergency Readiness Team

RAT:
"Remote access trojan," a malware that includes backdoor access for control over a targeted computer

INDUSTRY'S NEW ROLE

In Operation Blockbuster, Novetta identified the specific attack tools of a well-connected, globally significant attack group. Novetta and industry partners worked together to understand and devise ways to degrade the malware toolset, eroding the group's ability to use these tools for further harm. The industry team shared information and took decisive action to protect collective customers.

This sets a precedent for industry's new role in the changing dynamic of cyber defense. Industry is no longer only a watchdog. As the work behind Operation Blockbuster continues, Novetta demonstrates that elite security professionals with the right skills and talents, working collaboratively, can and should take decisive action not only to protect against attacks, but to fight back against attackers. These industry teams can provide customers with additional protection while educating the general public about modern cyber threats.

BUSINESS IMPLICATIONS

The Sony Pictures attack, and the long thread of related attacks documented in Operation Blockbuster, demonstrates that commercial enterprises are already living in a new era of cyber threats. As corporations' cyber footprints continue to grow, security operations are often unable to scale. Malicious threat actors like the Lazarus Group remain a step ahead. The urgency for building and maintaining a robust and evolving cybersecurity practice has never been greater. As an executive, you know it's your responsibility to maintain the integrity and security of your brand, and your customers' data. Learn how to better protect your enterprise. Download Operation Blockbuster to read the full story and remediation suggestions.

CONTACT NOVETTA:

- Technical and security questions, contact Novetta's Threat Research & Interdiction Group: **trig@novetta.com**
- For information on Novetta security services, solutions and products, email: **contact@novetta.com**

NOVETTA
7921 Jones Branch Drive, McLean, VA 22102
571.282.3000

DOWNLOAD THE FULL OPERATION BLOCKBUSTER REPORT AT:
www.OperationBlockbuster.com