National Cyber Investigative Joint Task Force

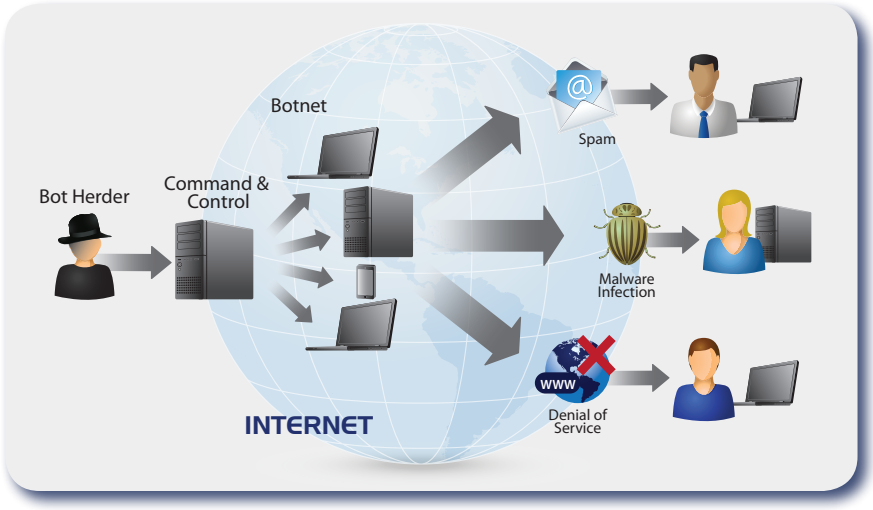
Operation Clean Slate

In the last several years, the use of malicious software (malware) by online criminals has emerged as a global cybersecurity threat. Of the available intrusion devices, the "bot," or Web robot, is particularly pervasive, allowing an attacker to take control remotely of a compromised computer or computers. Invisible to victims, these networks, called "botnets," can include hundreds of thousands of machines around the world, controlled by a cyber criminal, or "bot herder." Once in place, botnets are commonly used in distributed denial of service (DDoS) attacks, proxy and spam services, additional malware distribution, and for other organized criminal activity. Operation Clean Slate, spearheaded by the National Cyber Investigative Joint Task Force (NCIJTF), is a comprehensive, public/private effort engineered to eliminate the most significant botnets jeopardizing U.S. interests by targeting the criminal coders who create them.

Bots on the rise: The business of intrusion tools nets big criminal returns

Computer security firm Sophos estimates that 200,000 malware variants are created each day, many of which are sold or traded via Internet forums for use in building botnets. Industry experts estimate that bot infections affect nearly every market sector, including most of the top 20 Fortune 500 companies, as well as universities, hospitals, financial institutions, defense contractors, law enforcement, and nearly all levels of federal, state, and local government.

In addition to enabling more than a billion dollars in financial losses in just five years, botnet-related interruptions to Internet traffic and transactions derail the activities of government, companies, and individuals.



According to a 2012 survey by Neustar, 35 percent of businesses surveyed stated they would lose more than $10,000 per hour if a DDoS attack shut down their Internet site, and 13 percent of these reported potential losses would exceed $100,000 per hour.

Botnets can be used for covert intelligence collection, as well. In fact, terrorists or state-sponsored actors could use a botnet to attack Internet-based critical infrastructures directly, or as preparation of battle space before or during the preliminary stages of an attack. DDoS attacks might also be used as part of a political campaign to instigate fear, intimidation, or public embarrassment within the US financial sector.

Operation Clean Slate: A broad team effort designed to address a broad threat

The Operation Clean Slate initiative will incorporate all facets of the U.S. government (USG), international partners, major Internet service providers, the U.S. financial sector, and other private sector, cyber stakeholders.

Operation Clean Slate objectives:

- **Degrade or disrupt the actor's ability to exfiltrate sensitive information** from U.S. networks through arrests, by deploying a technical solution to interrupt the botnet, and by working with private sector partners to update security software that detects and damages the bot's malware.
- **Increase the actor's cost of business** by causing wasted time debugging failures, or forcing an actor to write new code for new botnet attacks. For an unsophisticated actor, the technique could disrupt an operation for days or weeks.
- **Seed uncertainty in the actor's cyber activity** by causing concern about potential or actual law enforcement action.

Partners and Roles

U.S. Government

- **The National Cyber Investigative Joint Task Force (NCIJTF)** will lead the initiative by coordinating all global facets of investigations and planned arrests, and share intelligence with all partners.
- **DOJ/Computer Crime and Intellectual Property Section (CCIPS) and National Security Division** will provide consultation and support on legal processes within the overall initiative. DOJ will consult with field offices to ensure proper legal process is executed according to the facts and evidence of each investigation.
- **DHS/National Cybersecurity and Communications Integration Center (NCCIC)** will be the lead agency for mitigation and recovery efforts, and will also be incorporated into intelligence support and prioritization of future targets and networks.
- **FBI Cyber Division (CyD)** will lead field office tactical efforts and coordinate global investigations and arrests through Legat offices. The Outreach Section, through its Cyber Initiative and Resource Fusion Unit (CIRFU) and Guardian Victims Analysis Unit (GVAU), will lead intelligence sharing with private-sector partners, participate in mitigation and recovery efforts, and take responsibility for victim notification.
- **Office of General Counsel Cyber Task Force** will advise the FBI/DOJ on all legal and policy implications of proposed operations, and will coordinate with other agency participants to ensure proposed operations are conducted in accordance with law and policy.
- **Internet Crime Complaint Center (IC3)** will filter incoming complaints to tag possible botnet traffic and will route such information to the analytical team.
- **National Security Agency (NSA)** will provide direct data on bonet threats seen from the international perspective. NSA will engage with the FBI field office working the botnet case, and will provide technical capabilities to that field office for target identification and botnet infrastructure. NSA may also assist with possible technical solutions for the bot networks, and may assist in mitigation planning depending upon the traffic and data identified.
- **U.S. Secret Service (USSS)** will coordinate with FBI efforts and investigations to deconflict investigative overlap. Specific bot cases may leverage both agencies' platforms and sources.

International

- **Europol and other international law enforcement partners** will be crucial in designing neutralization strategies and impacting the botnet threat. NCIJTF will manage these partnerships, directly coordinate arrests, and finalize mitigation efforts and results. International law enforcement partners will also provide input on future targeting and prioritization efforts.

Private Sector – Information Technology

- **Internet service providers, operating system companies, and antivirus companies** will provide direct data on bot threats witnessed from the industry perspective. They will assist in mitigation of bot networks, depending upon the traffic and data identified.
- **IT security research companies** will bring their targeting efforts and intelligence to identify bot networks and to propose possible technical solutions.
- **Internet Infrastructure Coalition (i2C)** will push appropriate intelligence to its member hosting companies and will provide information on potential bulletproof hosts.

Private Sector – Finance

- **Financial Services Information Sharing and Analysis Center (FS-ISAC)** will provide an avenue for publicizing arrests of bot networks to its member institutions.
- **Correspondent banks** will examine the flow of funds through their institutions from the U.S. to overseas subjects, and will assist in identifying fraudulent activity tied to specific data sources. When appropriate and possible, they will interrupt fraudulent financial transfers.
- **National Cyber-Forensics and Training Alliance (NCFTA)** member institutions will provide input from their experienced IT staff to help measure the impact of specific bot arrests.

The Operation Clean Slate initiative will move through four stages:

Phase I: Prioritize the Threats

The NCIJTF will lead prioritization of threats, and along with the FBI's Cyber Division, will enlist the expertise of its major USG partners to include NSA, DHS, USSS, and DOJ/CCIPS. Through robust liaison efforts, Operation Clean Slate will also utilize time-sensitive information from Five Eyes international intelligence sharing network (FVEY) and other international law enforcement partners, as well as from major internet service providers, antivirus makers, and other private-sector allies.

Coordination across these elements provides background and real-time intelligence on the most significant botnet actors, on significant infrastructure providers within the cyber underground, and in the identification of new trends within the community. The size, capabilities, and uses of a botnet are considered in developing the priority level, as well as in identifying the USG tools that can be used to mitigate and dismantle the threat.

Phase II: Identify the Actors

Once Operation Clean Slate identifies a priority botnet, the team will identify the specific actors: the coder who created the botnet, the "herders" who aggregate victim computers, and the users who deploy the botnet. In addition, the malware signatures being deployed via the botnet will be identified. This stage also includes identification of intended or actual victims.

Given the worldwide scope of the threat, the ongoing support of international and domestic public and private partners will continue to be invaluable to the FBI. Operation Clean Slate will use all tools at its disposal; such as online undercover operations, signals intelligence, source development, private-sector analysis, financial traces, and traditional criminal and national security investigative techniques.

A Case Study in Success

Coreflood Botnet Mitigation

- Millions affected worldwide, 800k in U.S., $20 million plus in damages
- Security partners helped to reverse engineer the bot infection and develop detection and removal signatures
- Multi-pronged approach took over the "command and control" network, mitigated infection, and provided victim notification
- 400 corporate victims and 32 ISPs notified, 90 foreign governments notified, 95% mitigation
- First DoJ approval of "minimal intrusion of victim computers for the greater good of end-users"
- Increased international awareness and partnerships

Phase III: Enact the Best Response

Discussions among Operation Clean Slate partners will help determine how to enact the best response to the botnet; which will vary depending upon the geographic locations of the actors, available domestic and international legal tools, and the possibility of designing and implementing a technical solution to disrupt the botnet. The menu of response options includes law enforcement action (arrests and search warrants), civil takeover (restraining order or injunctions), or signature sharing (updates with partners to enable improved security measures). The response strategy will always include an appropriate media/publicity component.

Phase IV: Implement Appropriate Neutralization and Mitigation

Operation Clean Slate will implement appropriate neutralization and mitigation with the assistance of the Department of Homeland Security (DHS) and private-sector partners. The mitigation strategy will be identified long before the arrest, as our private-sector partners require sufficient lead time to prepare for mitigation efforts, such as developing scripts for their call centers in preparation for offering specific short-term assistance to victims. The initiative will also work closely with antivirus companies to improve the technical protection available through commercial computer security programs.

Measuring the program's success

Specifically, Operation Clean Slate's objective is to eliminate the most significant botnet activity and increase the consequences for those who use botnets for terrorist purposes, intellectual property theft, or other criminal activities. The metrics used to define the operation's impact will include a variety of indicators and figures from public, private, and international partners working the threat. Given that no single agency or company tracks the number of botnets in existence, the number of victims impacted, or the dollar value of damages caused by all botnets, the initiative will harness multiple inputs to describe the results of its efforts.

According to a 2012 survey by Neustar, 35 percent of businesses surveyed stated they would lose more than $10,000 per hour if a DDoS attack shut down their Internet site, and 13 percent of these reported potential losses would exceed $100,000 per hour.

Some of this data will come from ISPs and antivirus companies, which may offer limited analysis on the amount of extra traffic caused by botnet attacks and the number of customers victimized. Input will also come from the financial sector, where prominent financial institutions are tracking codes tied to fraudulent fund transfers and may be able to identify successfully blocked criminal transfers.

Additionally, some FBI online undercover operations, U.S. intelligence community (USIC) partners, or private-sector researchers may be monitoring online chatter of bot herders and coders in criminal forums, and these conversations may reveal impacts of Clean Slate actions by reflecting unease on the part of criminal actors. Therefore, the overall success of the initiative will be measured by a confluence of all of these factors to examine patterns of botnet activity over time.

Carefully orchestrated to generate a substantial impact against the perpetrators and threats driving botnet attacks, Operation Clean Slate is expected to produce a measurable reduction in the bot-related hemorrhage of U.S. financial assets, traffic congestion across Internet services, and victimization risk to U.S. corporations and citizens.

For more information, contact your nearby FBI field office or visit www.fbi.gov.