IMMUNITY ADVERSARY SIMULATION

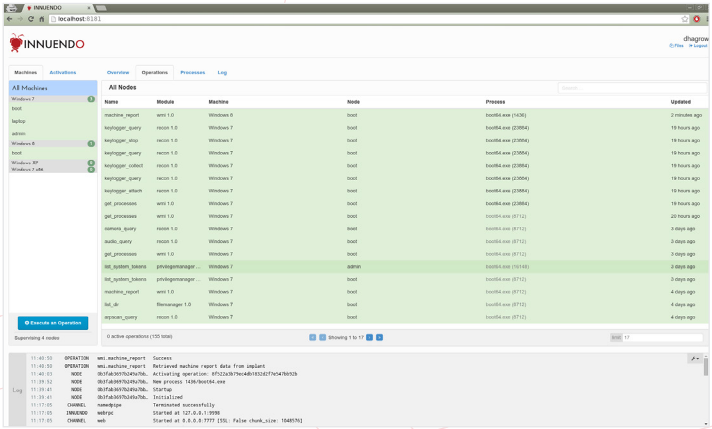
Has a full scope penetration test ever failed to compromise your network? When was the last time your red team did not succeed? The reality is that given sufficient time and resources a skilled attack team will always find a way into your infrastructure. This is why the cutting edge of network defense is shifting to an incident response model that revolves around an assumption of compromise. **You know you will get compromised**, now what?

IMMUNITY ADVERSARY SIMULATION allows you to model an advanced persistent threat from inside your infrastructure and evaluate how your security team will react to a real world offensive team that is active on your network and attempting to exfiltrate large amounts of data.

HOW IS IMMUNITY ADVERSARY SIMULATION DIFFERENT FROM PENETRATION TESTING?

+ It is strategy driven and goal oriented towards data exfiltration
+ It operates from an assumption of compromise: our team assumes the role of a competent and sophisticated threat actor that has already dug itself into your network
+ It establishes real world persistence inside your infrastructure thus providing real world indicators of compromise to your incident response team
+ It does not employ potentially destructive exploitation methodologies against production environments to establish access, so it is low-impact on day-to-day operations and safe to perform inside your actual infrastructure

IMMUNITY ADVERSARY SIMULATION is the next step in threat assessment and incident response preparedness. Recent history has shown that the modern enterprise has to maintain a security posture that operates under the assumption of compromise. You will get compromised at some point in time and acknowledging this fact helps you prepare for the next level of incident response: dealing with an active and potentially advanced attacker inside of your infrastructure.



Name	Module	Machine	Node	Process	Updated
machine_report	wmi 1.0	Windows 8	boot	boot64.exe (1436)	2 minutes ago
keylogger_query	recon 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
keylogger_stop	recon 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
keylogger_query	recon 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
keylogger_collect	recon 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
keylogger_query	recon 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
keylogger_attach	recon 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
get_processes	wmi 1.0	Windows 7	boot	boot64.exe (23884)	19 hours ago
get_processes	wmi 1.0	Windows 7	boot	boot64.exe (8712)	20 hours ago
camera_query	recon 1.0	Windows 7	boot	boot64.exe (8712)	3 days ago
audio_query	recon 1.0	Windows 7	boot	boot64.exe (8712)	3 days ago
get_processes	wmi 1.0	Windows 7	boot	boot64.exe (8712)	3 days ago
list_system_tokens	privilegemanager ...	Windows 7	admin	boot64.exe (16148)	3 days ago
list_system_tokens	privilegemanager ...	Windows 7	boot	boot64.exe (8712)	3 days ago
machine_report	wmi 1.0	Windows 7	boot	boot64.exe (8712)	4 days ago
list_dir	filemanager 1.0	Windows 7	boot	boot64.exe (8712)	4 days ago
arpscan_query	recon 1.0	Windows 7	boot	boot64.exe (8712)	4 days ago

0 active operations (155 total)

```
11:40:50  OPERATION  wmi.machine_report    Success
11:40:50  OPERATION  wmi.machine_report    Retrieved machine report data from implant
11:40:03    NODE     0b3fab3697b249a7bb..  Activating operation: 8f522a3b79ec4db1832d2f7e547bb92b
11:39:52    NODE     0b3fab3697b249a7bb..  New process 1436/boot64.exe
11:39:41    NODE     0b3fab3697b249a7bb..  Startup
11:39:41    NODE     0b3fab3697b249a7bb..  Initialized
11:17:05   CHANNEL   namedpipe             Terminated successfully
11:17:05  INNUENDO   webrpc                Started at 127.0.0.1:9998
11:17:05   CHANNEL   web                   Started at 0.0.0.0:7777 [SSL: False chunk_size: 1048576]
```

HOW IT WORKS

Immunity deploys INNUENDO based implants on designated systems. These implants, managed by the Immunity Adversary Simulation (IAS) team, operate at nation-state grade levels of sophistication, and communicate with their C2 servers using INNUENDO's flexible channel-stack technology. Examples of channels include DNS, ICMP, IMAP, SMTP, HTTP, and FTP, as well as customized data exfiltration channels tailored to your specific network conditions (e.g. externally facing corporate Wiki sites and in-house corporate messaging solutions). The Immunity Adversary Simulation team will set out to achieve a series of adversarial goals using this INNUENDO based shadow-infrastructure. Examples include large volume data exfiltration, lateral network movement and privilege escalation attacks. By doing this the IAS team generates real world indicators of compromise which are then used to prime your incident response team on how to recognize, interrupt, and prevent large volume data leaks out of your network.

To learn more about how IMMUNITY ADVERSARY SIMULATION can help improve your network security posture and incident response, please contact us at **admin@immunityinc.com** or give us a call at +1-786-220-0600.

Follow us on Twitter @immunityinc

IMMUNITY

1130 Washington Avenue – 8th Floor, Miami Beach, Florida 33139
Phone (786) 220-0600 | Fax (786) 513-8100 | admin@immunityinc.com | www.immunityinc.com