ThreatSTOP™

Customer Stories:

Earth Systems

“We had no idea all this malware was strangling our system and causing major problems.”

EARTH SYSTEMS

Earth Systems
San Luis Opisbo, CA

The problem:

- Infected with hundreds of malware but were unaware of them.
- Cisco router/firewall did not block the bots and Trojans.
- Cisco management console hard to use, dificult to manage.

www.threatstop.com
sales@threatstop.com
US: 760-542-1550

Customer overview:

Founded in 1969, Earth Systems is a geotechnical engineering and environmental company with 155 employees in 11 offices across western U.S. and China. Its customers range from public works, hospitals and schools to military facilities and renewable energy projects. Its IT infrastructure is comprised of a Windows Active Directory domain and Cisco router/firewall network supporting 180 desktops, servers and virtual machines. Its 10 remote offices use a VPN to connect to HQ and DSLs to directly connect to the Internet—a very typical architecture for SMEs.

Examining the issue:

The problem is that the Cisco 2821 router/firewall has “holes” that would allow malware to enter Earth System network. Rick Gaustad, Earth Systems’ CIO, had been one of ThreatSTOP’s earliest beta users, and he showed his logs to ThreatSTOP. Upon analysis, the logs showed that there were many bots, Trojans and other malware on machines inside EarthSystems.

Examining the Issue (continued):

“This was totally unbeknownst to me that there was all this malware that could cause significant problems for us. I just didn’t know it was there,” said Rick. “Cisco’s GUI is not user friendly; Cisco techs expect me to use their command line interface (CLI) to create logs within the device, which makes it very hard for me to find out what’s inside.

How ThreatStop solved it:

After deciding to implement ThreatSTOP, Rick discovered another problem. It turns out his Cisco router was incorrectly configured to support network objects, which made it impossible for ThreatSTOP to update the rules automatically. So instead of trying to fix it, it was decided that a Vyatta 514 appliance would be used in a transparent bridge mode to the Cisco, and ThreatSTOP will update its feeds to the Vyatta. “That worked like a charm. The ThreatSTOP people brought the Vyatta, installed it, and took a bunch of old Juniper Netscreen boxes in trade and I was immediately live on the ThreatSTOP service,” Rick said.

Results:

Today, Rick pulls up his daily ThreatSTOP log from the Web and sees immediately how many inbound and outbound blocks there are each day. The problems are easily identifiable, and by drilling down on the reports, Rick can see the details of each attack that enable him to fix the problem as well as have enough forensic data to prosecute if he chooses. “We had a couple of times when a couple of employees were doing Google searches, got infected by the Zeus and other bots that were trying to call home. As advertised, ThreatSTOP blocked the calls. We traced the problem to the machines in question, and cleaned them up,” Rick continued.

Additionally, ThreatSTOP reduced spam and recon bottraffic through its “cloak of invisibility” feature, which prompts malware perpetrators to move on and attack other sites because Rick’s network seems to have “disappeared” from the Internet.

“ThreatSTOP works great. We are attacked every day and it stops them. It gives me the ‘warm and fuzzies’ that I am protected. It’s well worth every penny.”

Richard Gaustad
VP/CIO, Earth Systems

ThreatSTOP™

The solution:

- Vyatta 514 appliance installed in bridge mode before the Cisco 2821 to implement ThreatSTOP.
- Daily web-based report shows inbound and outbound blocks and enables remedial actions.
- Reduced spam and recon bot traffic.

www.threatstop.com
sales@threatstop.com
US: 760-542-1550