Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations

Sathya Chandran Sundaramurthy
University of South Florida
Long Term Anthropological Study of Security Operation Centers (SOCs)

Sathya Chandran Sundaramurthy
University of South Florida

Xinming (Simon) Ou
University of South Florida

Alexandru G. Bardas
Kansas State University

Yuping Li
University of South Florida

Loai Zomlot
Kansas State University
(Alumnus)

Jacob Case
Kansas State University
(Alumnus)

Michael Wesch
Kansas State University

John McHugh
RedJack, LLC

Raj Rajagopalan
Honeywell ACS Labs
Can you check the client's / No access.
The IP tables was blocking the loopback interface and their tools couldn't communicate.
Did you document that?
Did you document that?
We need to help them.

But How?
Malware Incident Response
Malware Incident Response

Greetings

The following host(s) have been identified as likely compromised with the ZeroAccess Trojan.

<table>
<thead>
<tr>
<th>Inc #</th>
<th>description</th>
<th>address</th>
<th>timestmap in UTC</th>
<th>s-prt</th>
<th>dest-addr</th>
<th>d-prt</th>
</tr>
</thead>
</table>

All the data that we have for each observation is provided. If data such as source port, destination address, etc. is not provided, then we don't have that data. We may have additional observations collected during the reporting period, value depending on multiple factors (NATing, source port availability, etc.)

If you feel you've received this report in error, please let us know.

Additional information regarding ZeroAccess Trojan is provided below.

In order for the REN-ISAC to learn how we can best aid the education community with network security matters we'd greatly appreciate hearing back from you regarding action on this incident and how, if at all, this information proved useful.

Research and Education Networking ISAC
24x7 Watch Desk: +1(317)278-6630, scc@ren-isac.net
http://www.ren-isac.net
Malware Incident Response

Malware Incident Response
10 minutes/alert
10 minutes/alert
X 15 alerts/day
10 minutes/alert

X 15 alerts/day

= over 2 hours/day
Analyst Software, Skills (Tools)

Usefulness

Compliance

Creativity

Objective

Threat Detection & Mitigation

Showing ROI

Adherence

escalate
Usefulness

Software, Skills (Tools)

Compliance

Analyst

Objective

Creativity

Adherence

Threat Detection & Mitigation

Showing ROI

escalate
Firewall Logs

Access point Logs

ARP Logs

DHCP Logs

Point of Contacts
Firewall Logs

Access point Logs

ARP Logs

DHCP Logs

Indexed centralized Log Collection

Analyst

Point of Contacts
10 minutes / alert

↓

10 secs / alert
Before ...

Usefulness

Compliance

Software, Skills (Tools)

Objective

Analyst

Threat Detection & Mitigation

Showing ROI

Creativity

Adherence
After ...

Usefulness

Compliance

Creativity

Objective

Analyst

Software, Skills (Tools)

Adherence

Threat Detection & Mitigation

Showing ROI

Usefulness

Compliance

Creativity

Analyst

Software, Skills (Tools)

Objective

Adherence

Threat Detection & Mitigation

Showing ROI
After ...

Compliance

Usefulness

Software, Skills (Tools)

Creativity

Analyst

Objective

Threat Detection & Mitigation

Showing ROI

Adherence
After ...

Usefulness

Compliance

Software, Skills (Tools)

Objective

Creativity

Adherence

Analyst

Threat Detection & Mitigation

Showing ROI
The Saga Continues ...

Analyst

Software, Skills (Tools)

Analysts, Users, Management

Objective

Division of Labor

Specialty

Cross-domain Expertise
The deployment of our tool revealed more conflicts!
Conflicts Create Opportunities for Innovation!
Indexed centralized Log Collection

Access point Logs
Firewall Logs
ARP Logs
DHCP Logs
Web Server

Point of Contacts
Analyst
Software, Skills (Tools)

Analyst

Analysts, Users, Management

Objective

Division of Labor

Specialty

Cross-domain Expertise
A SOC is a dynamic system.

More conflicts will keep arising.

They have to be resolved on a continuous basis.
Activity Theory
(Engeström 1987)
These Insights are a result of

• 3.5 years of fieldwork

• At 4 different SOCs

• Involving 4 graduate students and 1 undergraduate student as fieldworkers

• Following systematic data analysis technique
  • Template analysis
Is that compliant?
Tensions & contradictions are gifts if we allow ourselves to see them.