Developing and Prototyping Honeypots

Julia Hornstein, Carly Hubert, Will Neuner, Joyce Thomas, Kelly Xu, Brock Davis

Project Overview

- Honeypots are decoy systems designed to attract and trap attackers.
- Configured to look identical to real systems, but not connected to any critical infrastructure
- Honeypots can be used to track the behavior of attackers
- We can analyze how hackers exploit honeypots which reveals a lot of information about an attacker's hacking techniques

Problem Statement

- Duke OIT faces billions of connections to Duke servers every day, many of these pose security threats as hackers scan networks looking for systems to infiltrate
- STINGAR (Shared Threat Intelligence for Network Gatekeeping and Automated Response) is a Duke developed platform containing honeypots that automatically detects and blocks network attacks and shares the generated threat intelligence in real time to other users

Project Outcomes

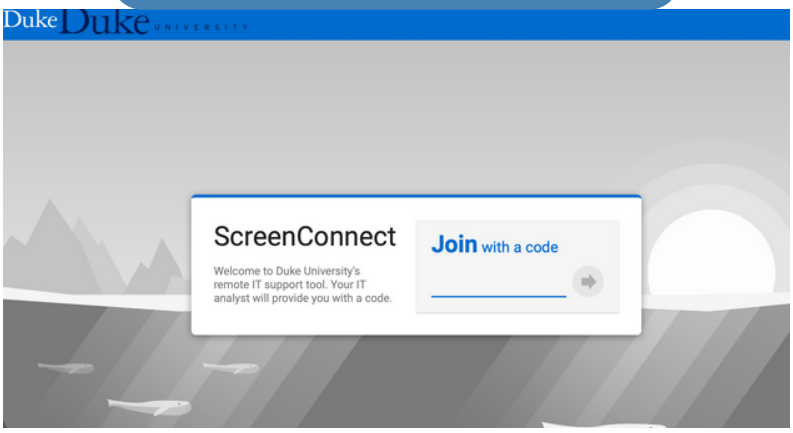
ScreenConnect

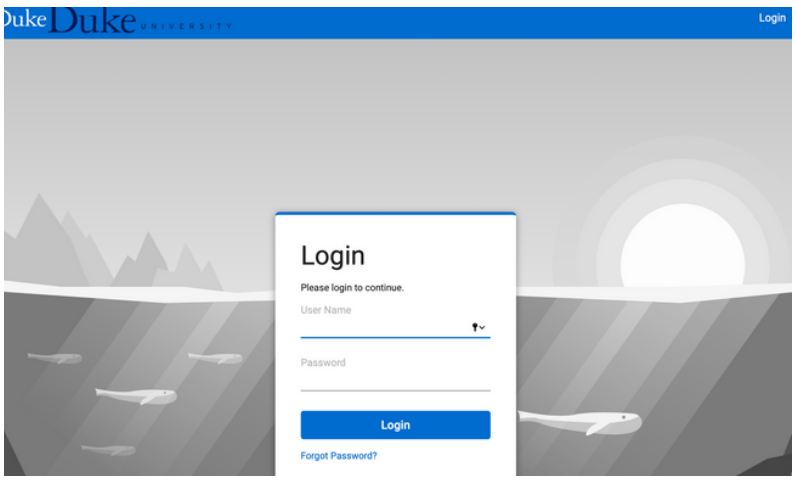
Duke's ScreenConnect page allows Duke OIT staff to remotely connect to client computers.

Threat analysis and prevention are necessary due to the powerful access granted by ScreenConnect.

A recent attack occurred using Duke credentials to access ScreenConnect.

Screenconnect web honeypot





KoiPot (SMTP)

Duke uses SMTP (simple mail transfer protocol) servers to send emails.

Duke mail servers have been targeted and abused for sending phishing attacks and spam emails.

SMTP is an outdated system with minimal security; it's easy for malicious actors to exploit.

Only a handful of the Duke OIT staff have access to the metadata of an email's true origins.

```
→  smtp-hp git:(simple_auth) ✗ telnet localhost 3000
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail-gw-39.oit.duke.edu ESMTP Thu, 27 Jul 2023 15:13:45 +0000
helo honeypots
250 mail-gw-39.oit.duke.edu ESMTP Hello [172.18.0.1], pleased to meet you
auth login
334 VXNlcm5hbWU6
YWJjMTIz
334 UGFzc3dvcmQ6
cGFzc3dvcmQ=
235 2.0.0 OK Authenticated
mail from: test@duke.edu
250 2.1.0 test@duke.edu... Sender ok
rcpt to: blah@gmail.com
250 2.1.5 blah@gmail.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
here is some mail.
click this link: https://www.youtube.com/watch?v=dQw4w9WgXcQ
.
250 2.0.0 44TBuOIA440140 Message accepted for delivery
thank you
500 5.5.1 Command unrecognized: "thank"
quit
mail-gw-39.oit.duke.edu ESMTP closing connection
Connection closed by foreign host.
```

Koipot SMTP server & JSON logs


```
"Client Address": ["172.18.0.1", 46340], "Time of connection": "2023/7/26 1
5:29.996439", "Time of termination": "2023/7/26 14:37:20.936565", "Username
["abc1"], "Password": ["password"], "Domain name": ["lalala"], "Mail from":
a@b.com"], "Rcpt to": ["c@d.com"], "Mail body": ["dGhpcyBpcyBzb25lIHRleHQuD
bGF5Lg0gLg0="], "Email Links": []}
"Client Address": ["172.18.0.1", 35080], "Time of connection": "2023/7/27 1
3:45.864054", "Time of termination": "2023/7/27 15:18:07.037410", "Username
["abc123"], "Password": ["password"], "Domain name": ["honeypots"], "Mail f
": ["test@duke.edu"], "Rcpt to": ["blah@gmail.com"], "Mail body": ["aGVyZSB
Bzb21lIG1haWwuDSBjbGljayB0aGlzIGxpbms6IGhYWHBzOi8vd3d3LnlvdXR1YmVbLl1jb20vd
Y2g/dj1kUXc0dzlXZ1hjUQ0gLg0="], "Email Links": ["hXXps://www.youtube[.]com/
ch?v=dQw4w9WgXcQ"]}
```