THE ANATOMY OF AN ATTACK *2015*

ALERT LOGIC®

ATTACK PATTERN STAGES

Attackers often use multiple tools in the same attack. The following is an example from the Alert Logic honeypot network.

INFILTRATION KILL CHAIN - Look for vulnerabilities

1 INFILTRATE

Spy-Y · DLoad-IK · Brambul-A · DwnLdr-KWB

PROBE KILL CHAIN - Steal passwords, keylogging, bypass authentication systems

2 PROBE

PWS-JJ · Agent-ZIU

EXPLOIT KILL CHAIN

3 EXPLOIT

Sality-D · Dropper-O

WHAT IS AN ATTACK?

An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network

WHY ATTACK?

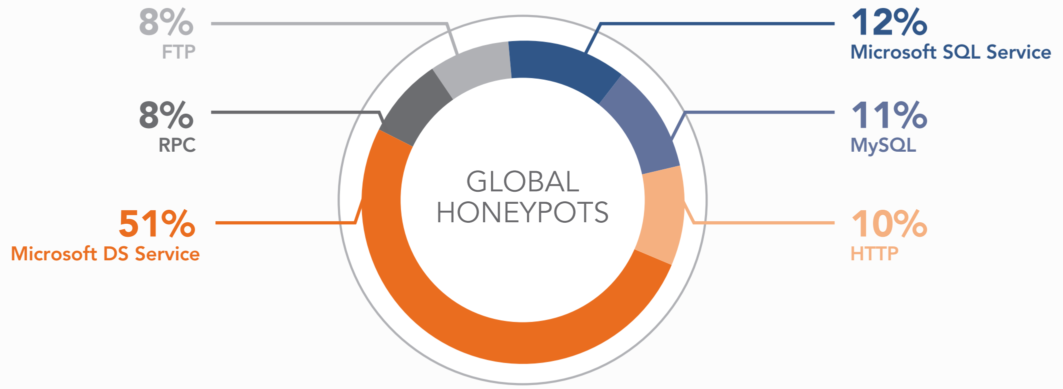
Financial gain
Cause fear
Maliciousness
Political motivation
Gain access to resources

HOW YOU CAN HELP YOURSELF

Secure your code
Create access management policies
Adopt a patch management approach
Review logs regularly
Build a security toolkit
Stay informed of the latest vulnerabilities
Understand your service providers' security

WHAT GETS ATTACKED?

While attackers will target almost any online service, in the Alert Logic global honeypot network, the most popular target was Microsoft Directory Services via port 445. Port 445 enables file sharing, so it's a popular target for transferring malicious content to servers.



PREVENTION

Protect yourself from specific attacks by pursuing the list below.

INFILTRATION

WEB APPLICATION FIREWALL
DETECT AND BLOCK ATTACKS

INTRUSION DETECTION
IDENTIFY BREACHES

FIREWALL*
BLOCK 445 TRAFFIC (IF PORT NOT IN USE)

PROBES

LOG MANAGEMENT
DETECT ATTEMPTED LOGGINGS

ANTI VIRUS*
DETECT PASSWORD-STEALING MALWARE

EXPLOITS

INTRUSION DETECTION
DETECT DATA LEAKAGE

NETFLOW
DETECT DATA TRANSFER

FILE INTEGRITY MANAGEMENT*
DETECT FILE MODIFICATIONS

MALWARE USED IN ATTACKS

Spy-Y
SCANS FOR PORT 445 & SENDS OUT EMAIL

DLoad-IK
TROJAN DROPPER, SCANS FOR PORTS 139 137 445

Brambul-A
TROJAN THAT SENDS OUT SMPT TRAFFIC, SCANS PORTS 139 445

DwnLdr-KWB
TROJAN EMAIL WORM, SCANS FOR PORT 445

PWS-JJ
PASSWORD STEALING MALWARE

Agent-ZIU
BYPASSES COMPUTER AUTHENTICATION SYSTEMS

Sality-D
SPREADS BY COPYING ITS CODE TO OTHER FILES OR PROGRAMS

Dropper-O
DOWNLOADS AND EXECUTES ADDITIONAL MALWARE

LEARN MORE www.alertlogic.com

*Not an Alertlogic Product Offering or Service