Explaining Worms and Virus

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

To expect the unexpected shows a thoroughly modern intellect.

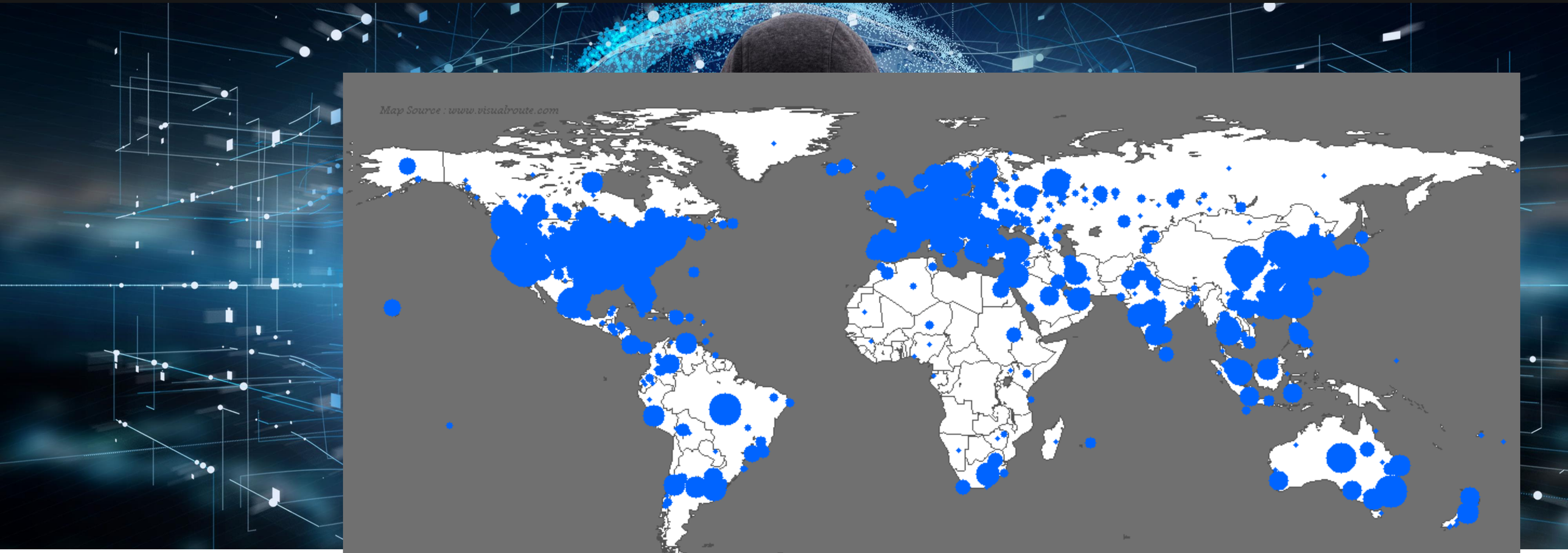
Oscar Wilde

What's the Difference?

Apples to Apples

What’s the Difference?

Back in the day..

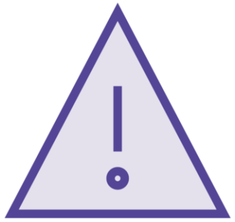


SQL Slammer

Based on PoC
Microsoft issued a patch
Caused routers to crash..and then

Viruses and worms are the scourge of modern computing

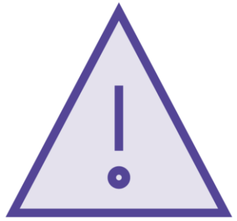
Other Characteristics of Viruses



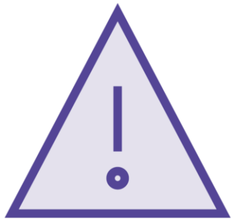
Infects other programs

Alters data

Transforms itself



Corrupts files and programs



Encrypts itself

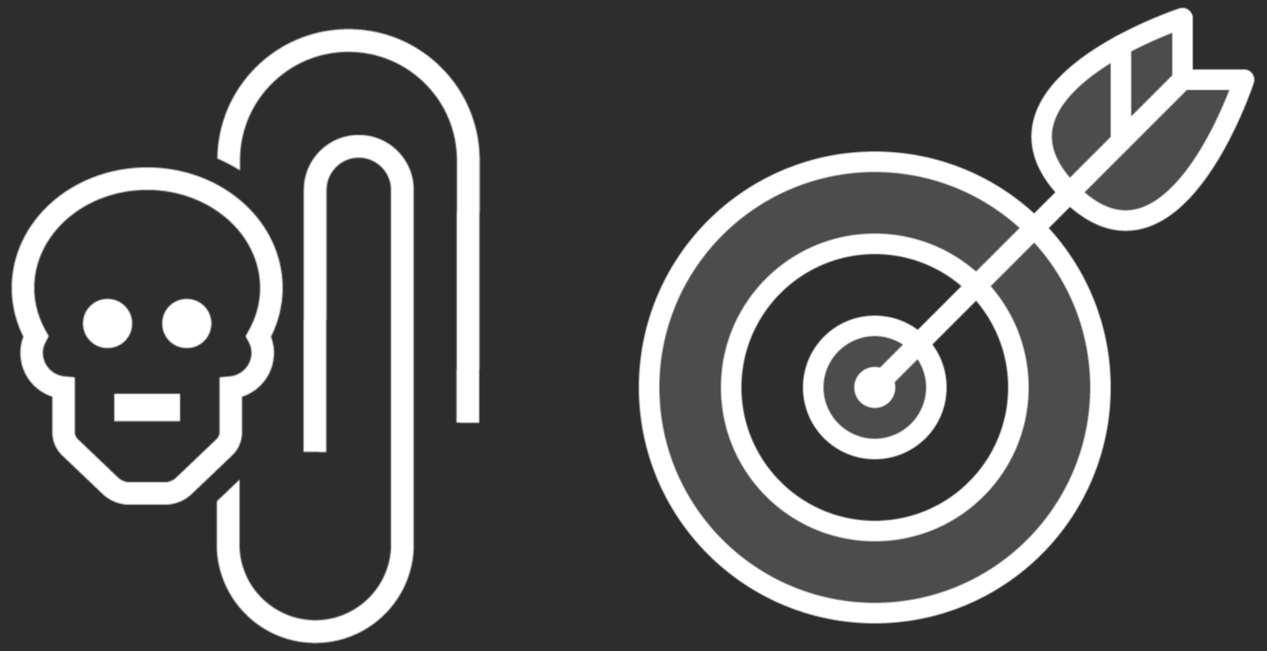
Replicates itself

Types of Viruses and Worms

Make the bad man go away

Types of Viruses

File



Prepending

Pending

Overwriting

Inserting

Types of Viruses

File

Cluster

Boot Sector

Back in my day..


A - ALK
AL - ANY
AP - BAB
BAC - BEA
BEB - BIS
CL - CON
COO - CZY
DA - DEC
DED - DIX
DO - DUN
GIB - GOP
GOR - GZ
HA
HE-HIL
HIM - HOY
LEG - LIN
LIS - LOV
LOW - MC
MAS - MEZ
P - PER
PES - POP
R - RH
RI - RZ
STA - SZ
T- THI
THO - TOZ
TRA - UNC
UND - VIS
VOI - WES
https://t.me/learningnets

Types of Viruses

File

Cluster

Boot Sector

Majority are distributed through PDFs

Continually rewriting itself

Types of Viruses

Cavity	**Installs in unoccupied space**

Types of Viruses

Cavity

Encryption

Types of Viruses

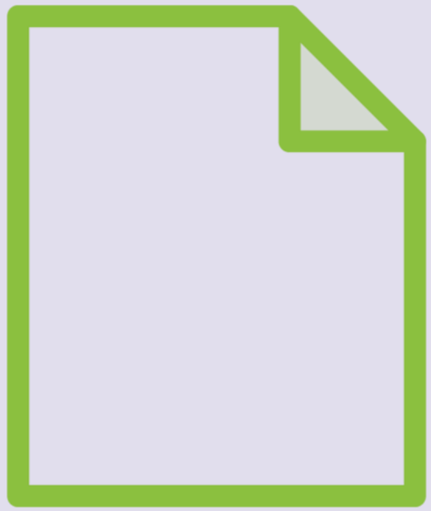
Cavity

Encryption

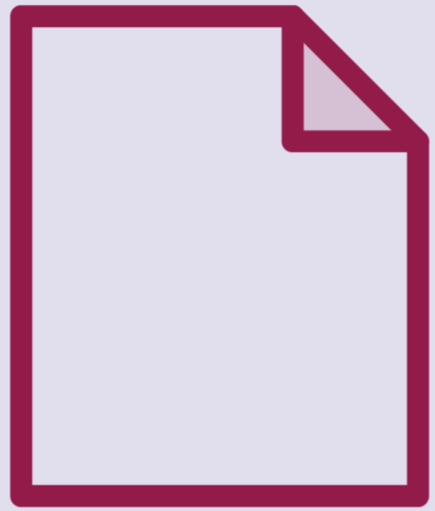
Camouflage

notepad.exe = > notepad.com

batman.com



batman.bat



batman.exe

Types of Viruses

Cavity

Encryption

Camouflage

Shell

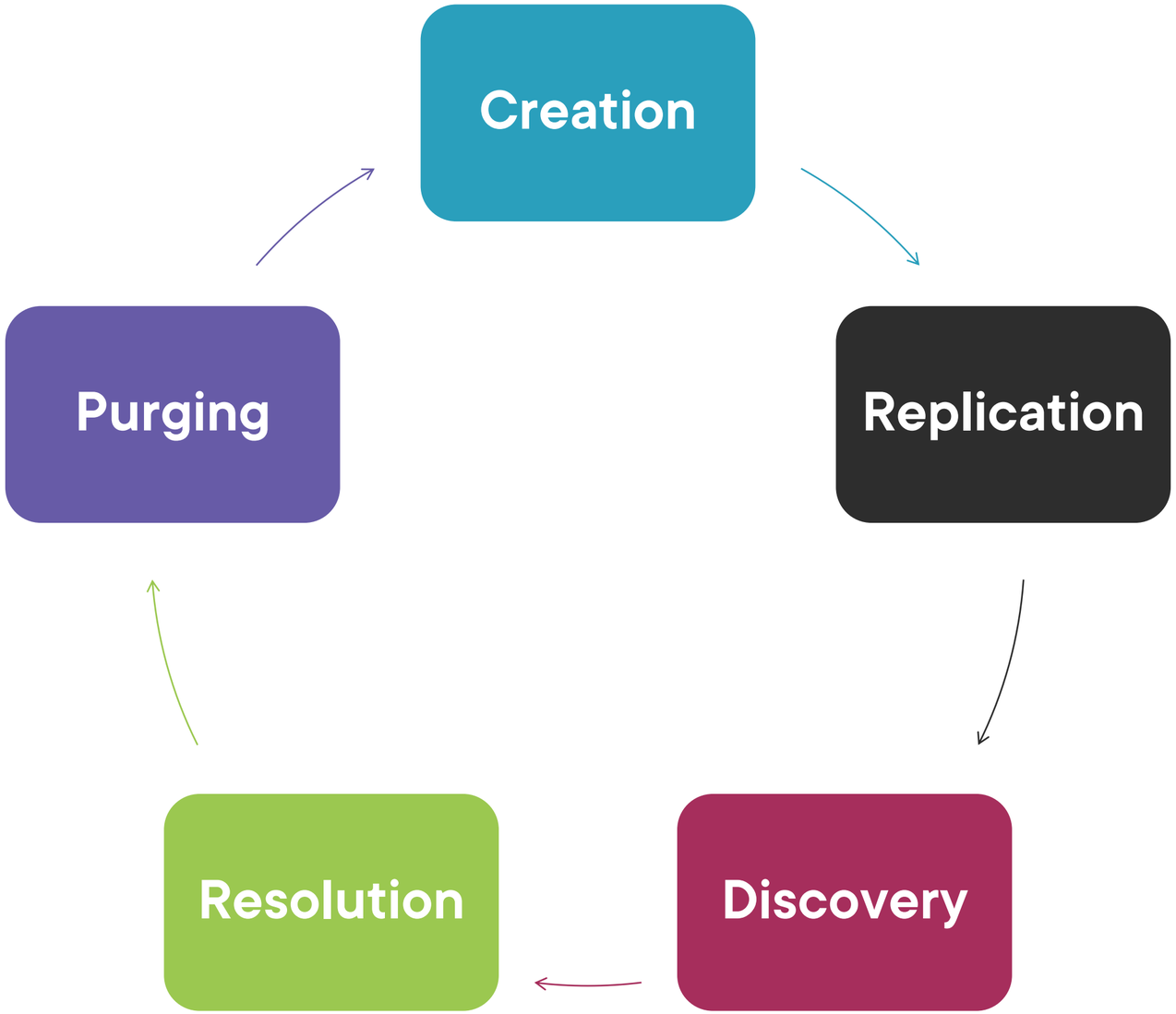
Tunneling

File extension

Demo

File extension

Lifecycle



Set Phasers to Stun!

Dale's Been Hacked

Dale's Been Hacked

Infection Phase

Needs an event

Replicates and attaches

Needs an event

-Setup files
-Startup
-TSR

Needs an event

Attack Phase

Corruption begins by deleting files

Altering file content

Execute tasks and camouflage

Most viruses have been written so that they don't execute until they've fully spread throughout the network

The Signs and Why

What Are the Signs?

Drive issues

Video issues

Memory issues

Apps and processes run slow

Computer freezes frequently

Files and folders are missing

Unwanted advertisements and pop-ups

Lack of storage space

Why?

Inflict damage on competitors network or computers

Vandalize intellectual property

Engage in cyber-terrorism

Distribute political messages

Realize financial benefits

Deployment

Round, Round, Get Around, I Get Around

How Does a Computer Get Infected?

Downloading infected files

Pirated software

Email attachments

Not updating OS/apps/anti-virus

How Does a Computer Get Infected?

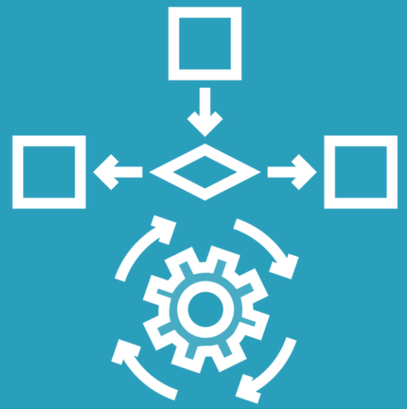
Plug-ins

Compromised sites

Spear-phishing sites

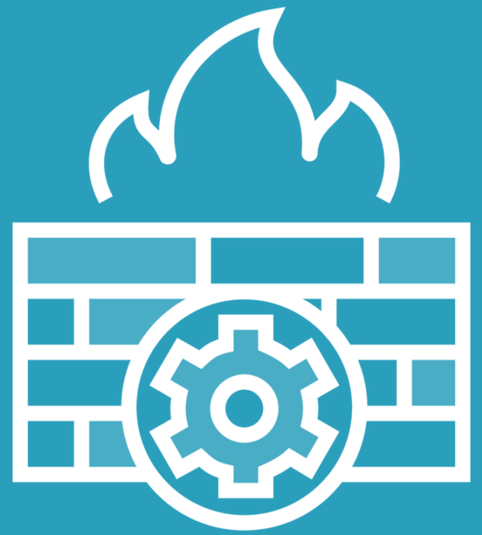
Click-jacking

How Does a Computer Get Infected?



Search Engine Optimization (SEO)

Incorrectly configured browser



Disabling a firewall

Connecting to an untrusted Wi-Fi network

Real? Fake? Does It Matter?

Trust Me - I Wouldn't Lie

IMPORTANT!!! YOUR COMPUTER IS PROBABLY INFECTED WITH A VIRUS. IN TURN, YOU HAVE SPREAD THIS VIRUS TO FRIENDS, FAMILY, AND CO-WORKERS JUST BY SENDING THEM EMAIL.

PLEASE READ AND PASS ON TO ANYONE TO WHOM YOU HAVE SENT EMAIL SINCE SEPTEMBER 11.

Why The Hoax?

Email headers

Delete legit files

Selling something

Contains virus attachments

Nothing is ever free

Learning Check

Learning Check

- Virus
- Overwriting
- Macro
- Metamorphic
- Camouflage

Learning Check

- File extension
- Tunneling
- Shell
- Plugin
- Cavity

Up Next:
Reviewing Fileless Malware