Chapter 6

Monday, August 14, 2023 11:37 AM

Understanding Threat Actors

advanced persistant threat **APT** - group of organized threat actors that targeted attacks on orgs over long period of time

state actors - sponsor APTs and target specific orgs

- China
- Iran
- NK
- Russia

Criminal syndicates - group of threat actors to do criminal activities for money

hacker - used to be pc nerd but now is same as threat actor

script kiddie - uses existing tech to launch attacks

hacktivist - launches attack as part

hacktivist - launches attack as part of activist movement

black hat - unauth hacker; criminal

white hat - auth hacker; law

gray hat - semi-auth; not for personal gain, intentions could be good

insider threat - someone w/ legit access to internal resources

- greed
- revenge

could also unknowingly be threat

ex: someone opens malicious script after phishing

competitor - any org in same industry want to gain proprietary info from org

ex: hire employees from other orgs

Attack vectors

attack vectors - paths that attackers . access to pcs/net

attack vectors - paths
use to gain access to pcs/net
these allow attackers exploit vuln

attackers target low-level orgs to gain
access to higher-level orgs

email
spam, malicious links/attachments
91% of all attacks start w/ email

Social media
often used to gather info

other attack vectors
- direct access VPN
- wireless, removable media, cloud
- supply chain

Shadow IT
any unauth systems or apps in org
added systems aren't managed and don't
have security controls

Determining Malware types

Determining Malware types

malware - malicious software installed unintentionally

infected sys
- run slow
- do unknown processes
- send emails
- reboot randomly

Viruses

virus - malicious code that attaches itself to a host app

host app must be exec for it to run

tries to replicate by finding other host apps to infect

payload - activated when host runs
deletes files, cause reboots, join pc to botnet, enable backdoor

worms

- self replicating malware; travels

Worms

worm - self replicating malware
through net w/out user action
resides in memory
consume net bandwidth

Logic Bomb

logic bomb - string of code embedded in app or script that exec in response to event

Backdoors

backdoor - provides another way of accessing system
often created w/ malware
created by devs for testing

account management policies prevent ex-employees from creating them

Trojans

trojan - looks like something legit but is malicious

can come as
- pirated software
. game
. utility

drive-by download - web server has malicious code that attempts to download when user visits
- attackers compromise site
- install trojan to code
- trick users into visiting
- trojan tries to install or visit

rogueware - or scareware; acts as free antivirus
says through message or webpage that malware detected
does "scan" and says to pay to get rid of them
may also install backdoor
extensions can also install

web browser extensions can also install

Remote access Trojan

RAT – allows attackers to control system remotely

growing trend to deliver through portable executable PE files

PE32 PE64

often compressed in .tar.gz files

can keylog

look to spread across net

keyloggers

Keyloggers – attempt to capture keystrokes

often saved to file

software & hardware

ex: USB keylogger

2FA thwarts because even if attacker steals pword, wont be useful

Spyware

spyware - software installed on user's systems without awareness or consent

monitors users pc, sends info to 3rd party

spyware activity

- change user's home page
- redirect browsed
- install add software

privacy-invasive spyware - tries to separate users from their money using data-harvesting

impersonate user and empty bank account

Rootkit

rootkit - single or group of programs that hides that system has been infected

user may expect something wrong but virus cases show nothing

Modify internal OS processes and system files like Registry

Sometimes modify system access

root-level access - same level of access as OS

hooked processes - intercept sys-level function calls, events, or messages

prevents antivirus from communicating with OS

antivirus can detect hooks by looking at RAM

booting in safe mode can help prevent

Bots and botnets

bots - software robots

botnet - combines multiple pcs that act as software bots and function together in a net

"serve" one central system or bot

herder - criminals who manage

"server" are ... herder - criminals who ... botnet

command and control

Command and control

command and control - resource that sends instructions to infected botnet pcs

can also be used in ransomware

internet relay chat IRC were used in early botnets

send commands out

some criminals migrated to P2P botnets - each infected sys looks for others to connect to

each sys acts as command and control sys for others

no central command and control

Ransomware and Cryptomalware

... control of system

Ransomware and ...ll

ransomware - take control of system and lock out user

crypto-malware - encrypt data and prevent access

almost all ransomware uses crypto techniques

Potentially Unwanted Programs

PUP - programs a user may not want after downloading another program

some are legit, others are malware

many of them are **browser hijackers** that make unwanted changes to web browser

Fileless Virus

fileless virus/malware - malicious software that runs in memory

memory code injection - inject code into legit apps using vulns

Java, adobe, PowerShell

Java, adobe, PowerShell

Script-based techniques

ex: using encrypted code that made it hard to detect

Windows registry manipulation

write and execute code into the Registry

can also be injected into **vCards** - elec business cards

Potential Indicators of a Malware Attack

- **Extra traffic**
  on net
- **data exfiltration**
- **encrypted traffic**
  DLP cant read encrypted traffic
  large amounts can be a sign
- **traffic to specific IPs**
- **outgoing spam**
  the sign pc is now in botnet

- outgoing [illegible]
  could be sign pc is now in botnet

Recognizing Common Attacks

Social Engineering

use social tactics to gain info

common methods

- flattery
- Authority
- encourage to do risky action
- encourage to reveal sensitive info
- impersonate someone
- tailgate

Impersonation

impersonate known entity to trick someone into revealing sensitive info

Shoulder Surfing

looking over the shoulder to gain info

- office near payment area, ...

in office, near payment area, ...

screen protectors

Tricking users with hoaxes

hoax - message, often email, telling of impending doom/virus/etc.

try to convince to delete files or change system configs

Tailgating and Access control vestibules

tailgating - following someone to gain unauth access

access control vestibule (mantrap) - room or building w/ large buffer area between secure/unsecure areas

guards, turnstile, ...

Dumpster Diving

search through trash to gain info

need to burn or shred PII docs

Zero-Day Vulnerabilities

Zero-Day Vulnerabilities

Zero-day - vulnerability unknown to trusted sources

Watering Hole Attacks

attempt to discover sites a group of people typically visit then compromise it to infect users

APTs use this

Typo squatting

URL Hijacking - buying domain name close to legit domain

reasons to use

- host malicious site
- earn ad revenue
- reselling the domain

Eliciting Information

Elicitation - getting info w/out asking for it

active listening

reflective questioning
repeat statement as question

false statements
say false statement hoping
target corrects

bracketing
use a range of numbers to try
to get attacker to correct

Pretexting and Prepending

pretexting and prepending are similar

pretext is ficticious scenario added
to convo to make request more
believable

ex: pretext = I'm a worker for
— vendor

Identity Theft and Fraud

identity theft - someone steals
PI from you

— stolen identity to

can then use stolen identity to commit identity fraud

apply for loan, file false tax return, send fake bills

Invoice scams

try to trick people into paying for goods and services they didnt request

ads, renew domain, unpaid bill

usually email or regular mail

Credential Harvesting

collect uname/pword

send email claiming problem w/ account

click link and enter creds

malware can also do this with keyloggers and screenshots

Reconnaissance

gather as much info as possible

gather as much
on target

open-source and phone-calls/visits

Influence campaigns

use hybrid warfare and social media to influence pubic perception

hybrid warfare - military strat that blends conentional warfare w/ unconventional methods

social media is popular outlet

Attacks via Email and Phone

Spam, phishing, smishing, vishing, spear phishing, whaling

Spam

unwanted or unsolicited email

mostly harmless ads, but can also be malicious

agreeing to terms typically also means [illegible] partners to

agreeing to terms typically ...
you're allowing their partners to send you email

criminals may use opt out buttons to confirm your email is valid

Spam over Instant Messaging

SPIM - unwanted messages over IM

bypasses typical antivirus and spam filters

Phishing

sending email to users w/ purpose of tricking them into reveal PI or click link

make effort to try to mock legit site

Beware of email from Friends

criminals use social media to impersonate your friends

... Malware

Phishing to install Malware

ex: fake email from news site but popup saying adobe flash is outdated and needs to be updated

Phishing to Validate Email Addresses

beacon - link in email that links to image stored on internet server

includes unique code that ids receiver's email

- must retrieve image from web server
- when server hosting image receives request it marks user's email as valid

this is why images aren't loaded in emails

Phishing to get Money

request for money for supposed money

request [illegible]

in return

ask for bank info

lottery scams

Spear Phishing

targeted form of phishing

- employees
- customers
- ...

digital signatures help prevent attackers from targeting employees by impersonating CEO or exec

Whaling

Spear phishing for high level targets

could be from better business bureau or justice dept

could be via phone

Vishing

using phone system

use VoIP to spoof caller ID

uses VoIP to spoof caller

evoke urgency with "warnings"

Smishing

SMS + phishing

some may have malicious attachments

some trick you into bypassing 2FA

One click Lets them In

one click from user can give attacker access to net

attacker can be anywhere in world only needs internet

attackers servers can be their own or could be in another country

could be using botnet

Steps in an attack

1. Use OSINT to identify target

social media

to learn about

social media
use phone call(s)/email to learn about org

2. Make spear phishing email with malicious link/attachment
usually for drive-by download
also could lead to cred farming
link

3. send email
4. user clicks link or attachment
5. user info is sent to attacker
could be done through site or by downloaded RAT
6. Attacker uses creds to access targeted system

lateral movement - uses infected system to move across net
typically use Windows management instrumentation WMI and Powershell

Powershell

7. use privilege escalation
   infected sys may not have perms
   use escalation to infect other systems and create backdoor accounts

8. Malware searches for data within the network
   emails / files

9. Gathers data and divides into encrypted chunks

10. Encrypted chunks are exfiltrated

Blocking Malware and Other Attacks

common controls to protect against malware

- spam filter on mail gateways
  some nets route traffic through another device to filter
- anti-malware software on mail gateways
  ... attachments

- anti-malware software
  detect malware in attachments
- all systems
  all systems need anti-malware
- boundaries and firewalls
  tools to detect like in UTM

Spam Filters

defense in depth
UTM, email server, user client all have spam filters

Antivirus and anti-malware software

most antivirus also blocks malware

- viruses
- worms
- trojans
- rootkits
- spyware
- adware

antivirus does realtime protection, scheduled + manual scans

Signature-based Detection

data definitions - define

Signature-Based

Signatures or data definitions - define patterns and antivirus scans files for matches

blocks or quarantines matches

Heuristic-Based Detection

attempts to detect previously unknown viruses

runs questionable code in a sandbox

ex: polymorphic malware adds variations to files when it copies

very unusual for apps to do this

File Integrity Monitors

file integrity monitors - detect modified system files

calcs hashes on system files for a baseline

changes to these files often mean rootkits

rootkits

Cuckoo Sandbox

Cuckoo Sandbox - open-source automated software analysis system

submit files for it to run in VM sandbox

Why Social Engineering Works

psychology-based principles to increase effectiveness

Authority

Impersonation

pretend to work for org

impersonate execs

Whaling

send execs legal docs

Visiting

use phone to impersonate

Intimidation

bullying combined w/ impersonation

Intimidation

bullying combined w/ impersonation

Consensus

websites w/ fake testimonials

bait for trojans

Scarcity

ex: exclusive access to sold out item

Urgency

ransomware, phishing, vishing, whaling

taking the need for immediate action

Familiarity

build rapport with victim

shoulder surfing is more acceptable if victim knows attacker

same with tailgating

Trust

build trust w/ victim over time

Threat Intelligence Sources

OSINT - gather info on targets

- websites
- social media

Closed/proprietary intelligence - trade secrets and IP

Common types of OSINT

- Vulnerability Databases
  - NVD
  - CVE
- Trusted Automated eXchange of Indicator Information TAXII
- Structured threat information expression STIX
  - What to share
  - How to share
- Automated indicator sharing
  - AIS
    - CISA maintained for exchange

CISA maintained
of threat indicators

- Dark web
- public/private info sharing centers
- indicators of compromise
- predictive analysis
  predict what attackers will do next
- Threat maps
  visual rep of active threats
  replay of recent attacks

  amon

  RedLegg

- File/code repos
  Awesome threat intelligence

Assessment Notes

sophisticated + likely from

1. Sophisticated + likely [illegible]
foreign country

APT

2. Attacker purchased exploit online
script kiddie

3. pretexting = call from someone
saying they are a rep for
vendor...

4. Zero-day = previously unknown

5. ransomware = unable to access data
request for payment

6. files lost after someone left
company

logic bomb

7. Programmed ability to login w/
account only known to programer

account only

backdoor

8. Abnormal activity, connect to sys outside org using uncommon ports, hidden processes

rootkit

9. Home page and default search engine changed

PUP

10. Sus activity from Powershell

fileless virus

11. Using cards and scanning prevents

impersonation

12. [illegible] w/ PII prevents

12. Burn docs w/ PII prevents

dumpster diving

13. Pretexting and trying to find out what OS servers use

evel call, report to supervisor, investigate

14. CFO gets email from "CEO" asking for money

whaling

15. Cant find popular phone in stock get email ad w/ malware

scarcity