NAME- ANMOL KANT

LET'S TALK ABOUT SOME NEW ATTACKS WHICH RECENTLY COME IN MARKET…..

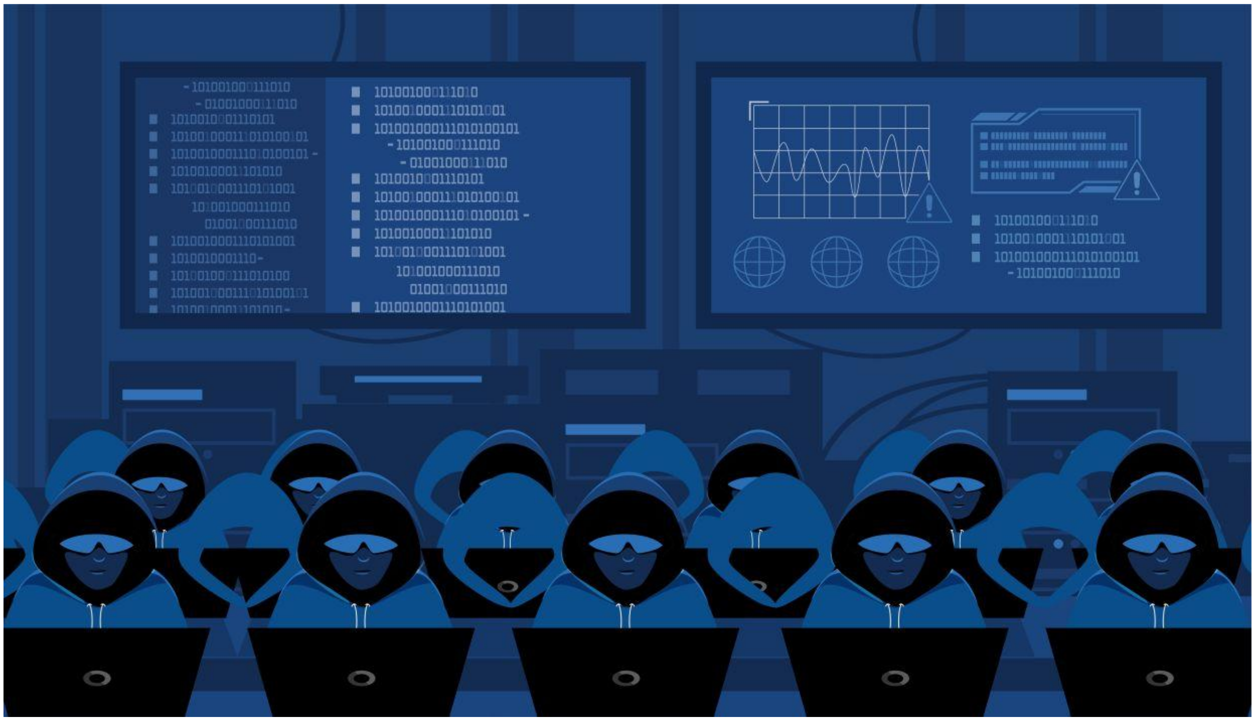
CYBERCRIMINALS ARE CONTINUALLY UPPING THE COMPLEXITY AND SEVERITY OF THEIR ATTACKS. HACKERS HAVE NOW BAKED AGILITY INTO THEIR DNA IN AN ENDLESS DRIVE TO EVOLVE TACTICS AND THROW EVER MORE NASTY SURPRISES AT UNSUSPECTING VICTIMS AND DEFENDERS ALIKE.

TODAY, THE HACKERS' EFFORTS AND ATTACK METHODS ARE INCREASINGLY TARGETED AND COMPLEX, MEANING AWARENESS, VIGILANCE, AND EDUCATION ARE VITAL WEAPONS AND OUR MOST CRITICAL LINE OF DEFENSE. EVERY DAY 450,000 NEW PIECES OF MALWARE ARE DETECTED, AND 3.4 BILLION PHISHING EMAILS HIT INBOXES. ATTACKS OF THIS NATURE HAVE BECOME ALL THE MORE PREVALENT, MORE SOPHISTICATED AND

HARDER TO DETECT. COMMONPLACE IN NATURE, THESE ARE THE ATTACK TYPES THAT HAVE COMMANDED MEDIA ATTENTION AND RALLIED CALLS FOR TARGETED AND COORDINATED PLANS TO STOP HACKERS DEAD IN THEIR TRACKS.

BUT WHILE THESE KEY TECHNIQUES IN THE HACKER SKILL SET LIKE MALWARE, PHISHING AND SQL INJECTION ARE EVER PRESENT YEAR AFTER YEAR, OTHER TECHNIQUES COME FRESH OUT OF THE BOX DESIGNED TO CATCH US –AND EVEN OUR BEST DEFENSE MEASURES- COMPLETELY OFF GUARD.

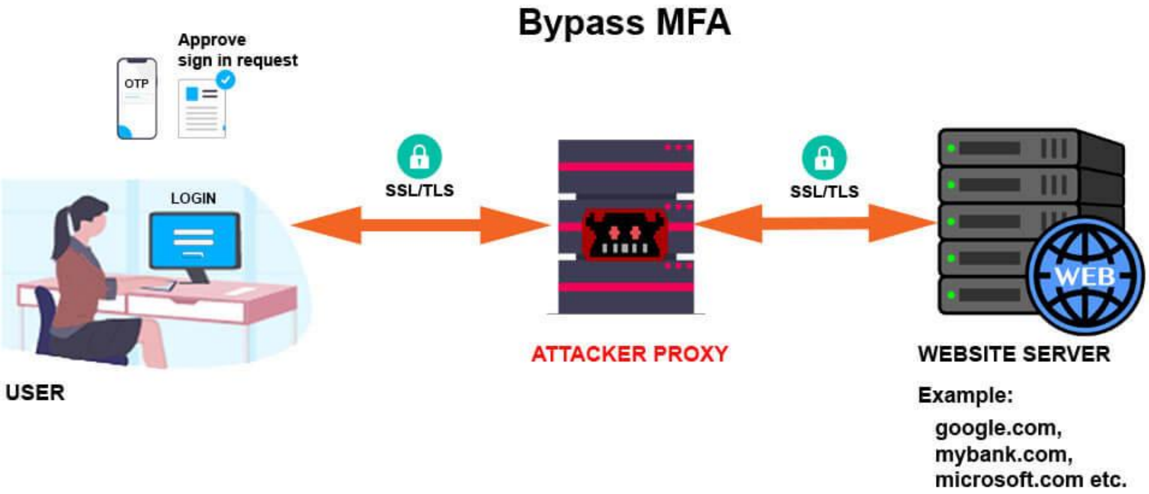
1) LIVING OF THE CLOUD



Seeing as how the cloud has become part of our everyday lives, adversaries are targeting cloud environments more than ever. While living off the land attack tactics continue to be in use, our cloudy present state has drawn adversaries up into the clouds as well.

Bad actors target cloud environments with these attacks because this tactic is cheap and easy to set up, deceives users and defenders by blending in with legitimate cloud services, and more easily bypasses firewalls and proxies. Adversaries know that users recognize cloud infrastructure. To detect and respond to these attack methods, adopt a mindset of "Know normal, find evil." In other words, know what is normal for your environment so that when something anomalous occurs, it's easier to identify it as a potential incident. Other approaches that will help you get ahead of these attacks include putting more resources into user education and working with cloud providers by reporting abuse of their platforms and brands.

2) MFA BYPASS



THERE IS CONTINUED MOVEMENT AWAY FROM USING MULTIPLE USE PASSWORDS AND TOWARDS ADOPTING MULTIFACTOR AUTHENTICATION (MFA), PASSKEYS, FIDO 2 AUTHENTICATION AND OTHER ADDITIONAL LAYERS OF SECURITY. COMPANIES LIKE APPLE AND GOOGLE ARE ALSO DEVELOPING THEIR OWN AUTHENTICATION TOKEN SYSTEMS.

THIS WILL ALL LEAD TO A BADLY NEEDED INCREASE IN SECURITY BUT ALSO RESULT IN AN EXPLOSION OF ATTACKS THAT AIM TO BYPASS SUCH MFA APPROACHES, INCLUDING USING STALKERWARE TO TAKE ADVANTAGE OF COMPANY EXECUTIVES AND BOARD OF DIRECTORS' USE OF MOBILE PHONES TO RECORD THEIR KEYSTROKES AND INTERACTIONS.

WITH AN MFA BYPASS TECHNIQUE, A LIKELY SCENARIO IS THAT AN ADVERSARY GAINS ACCESS TO A USER ACCOUNT THAT WASN'T PROPERLY DISABLED AND RE-ENROLLS THEIR ILLEGITIMATE DEVICE SO THAT THEY CAN BYPASS MULTI-FACTOR AUTHENTICATION.

BUT DESPITE CONCERNS WE SHOULD KEEP USING MFA. JUST LIKE THE FIRST TECHNIQUE, THE KEY TO GETTING AHEAD OF THIS CYBER-ATTACK TACTIC IS TO CHANNEL THAT SAME “KNOW NORMAL, FIND EVIL” MINDSET. COUNTER-MEASURES INVOLVE MONITORING FOR UNUSUAL USER BEHAVIORS AND LOGIN SOURCES AS WELL AS ENSURING THAT ALL INACTIVE ACCOUNTS ARE DISABLED UNIFORMLY ON ACTIVE DIRECTORY AND MFA SYSTEMS.

3) GHOST BACKUP

OUR THIRD MOST DANGEROUS ATTACK TECHNIQUE IS SOMETHING THAT WE REFER TO AS THE SPOOKY SOUNDING “GHOST BACKUP” ATTACKS.

WITH THIS APPROACH, AN ATTACKER FIRST BREACHES A BACKUP SYSTEM OR CONTROLLER, THEN ADDS A MALICIOUS BACKUP JOB THAT EXFILTRATES DATA TO THEIR OWN ATTACKER-CONTROLLED STORAGE. THIS ALLOWS THE HACKER TO RECONFIGURE YOUR BACKUP SOFTWARE TO EITHER STEAL PARTICULAR FILES OR TO CONFIGURE THEIR OWN BACKUP DESTINATION, SO THEY HAVE ACCESS TO ALL OF YOUR FILES. THE ATTACKER MAY ALSO USE

THE SAME CLOUD INFRASTRUCTURE WHICH MAKES DETECTION EXTREMELY CHALLENGING ESPECIALLY IF A HIGH VOLUME OF FILES IS NOT PULLED.

PRACTICING GOOD BACKUP SECURITY INCLUDES:

PERFORMING REGULAR INVENTORYING WHERE YOUR BACKUPS ARE, MONITORING AS CLOSELY AS THE OTHER SOFTWARE YOU ARE MANAGING

IMPLEMENTING DATA RETENTION POLICIES

ENSURING THERE IS A PLAN IN PLACE TO PATCH AGENTS

SECURING ACCESS TO THE CENTRAL MANAGEMENT CONSOLE

DEPLOYING END-TO-END ENCRYPTION, INCLUDING ENCRYPTION AT REST, IN PARTICULAR FOR OFF-SITE BACKUPS

4) STALKERWARE

WE ALL DESERVE TO ENJOY PRIVACY AND FULL PEACE OF MIND ACROSS OUR ONLINE LIVES SO IT'S IMPORTANT TO ENSURE OUR COMPUTERS, PHONES AND INTERNET DEVICES ARE FREE FROM PRYING EYES. THE SCOURGE OF STALKERWARE - SOFTWARE, APPS, AND DEVICES THAT FACILITATE CYBERSTALKING- IS BY NO MEANS A NEW TACTIC BUT THIS FORM OF MALWARE IS ON THE RISE AND RISKING VERY SERIOUS REAL-WORLD OUTCOMES.

WHILE MOBILE PHONES ARE MORE SECURE THAN DESKTOPS, WE WILL ALSO SEE A GREATER VOLUME OF STALKERWARE INCLUDED IN DOWNLOADED APPS THAT TARGET CONSUMERS. PEGASUS IS A KEY EXAMPLE OF THIS THREAT, WHICH CAN INSTALL ITSELF ON IOS AND ANDROID DEVICES WITH

ZERO CLICKS. HACKERS ARE ALSO CREATING MALICIOUS STALKERWARE APPS AND HIDING THEM IN APP STORES. AS PEOPLE BECOME MORE ACCUSTOMED TO DOWNLOADING FAMILY TRACKING SOFTWARE AND GIVING AWAY APP PERMISSIONS, THE RISK OF HAVING THEIR KEYSTROKES, LOCATIONS, VOICE, AND EVEN PHOTOS AND VIDEOS RECORDED FOR FINANCIAL THEFT AND OTHER NEFARIOUS PURPOSES WILL ALSO INCREASE.

CONSIDER SOPHISTICATED MOBILE MALWARE THAT SELF-INSTALLS AND SELF-DESTRUCTS. ZERO-CLICK EXPLOITS FOR IOS AND ANDROID ALLOWS BAD ACTORS TO GET IN AND GET OUT UNDETECTED, LEAVING LITTLE TO NO TRACE BEHIND THAT IS RECOVERABLE VIA FORENSIC ANALYSIS.

STALKERWARE IS STEALTHY BE DESIGNED AND MADE TO GO UNDETECTED BUT AWARENESS, VIGILANCE, AND MAKING STRONG SECURITY PRACTICES ROUTINE CAN ALL HELP TO KEEP US SAFE. SIMPLY PUT, CYBER HYGIENE MATTERS.

A FEW TACTICS WE SHOULD ALL ADOPT INCLUDE:

CHANGING PASSWORDS ON ALL DEVICES REGULARLY

REBOOTING DEVICES FREQUENTLY

NEVER CLICK ON RANDOM LINKS

5) CYBER WARFARE

IN TODAY’S POLITICAL ENVIRONMENT WITH INCREASING GLOBAL TENSIONS, SUCH AS WITH THE SITUATION IN RUSSIA AND UKRAINE, ATTACKS THAT SEEM MORE LIKELY TO MAKE UP THE PLOT OF A JAMES BOND MOVIE ARE, IN FACT, VERY REAL POSSIBILITIES. THE BOUNDARIES OF CIVILIAN AND MILITARY BLUR AND THE INTERNET AND APPS CAN FUNDAMENTALLY CHANGE INTELLIGENCE AND MILITARY OUTCOMES. JUST LOOK TO CIVILIAN COMPANY STARLINK’S $80 MILLION INVESTMENT IN UKRAINE'S COMMUNICATIONS INFRASTRUCTURE AS AN EXAMPLE.

BE AWARE THAT WITH SUCH LINES BLURRING AND GEOPOLITICAL TENSIONS BEING WHAT THEY ARE CURRENTLY, WE RUN THE RISK OF HAVING A SINGLE

BAD ACTOR DECIDE THEY'RE GOING TO SUPPORT THAT WAR, BUT FROM THEIR BASEMENT. THERE’S A NEW DIGITAL HIGH GROUND, IN WHICH OPEN-SOURCE, PUBLICLY WRITTEN TECHNOLOGIES CAN BE LEVERAGED IN MILITARY OPERATIONS.