**All below rules are available on** [**https://rules.emergingthreats.net/open/suricata-5.0/emerging-all.rules**](https://rules.emergingthreats.net/open/suricata-5.0/emerging-all.rules)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No** | **Date** | **ET OPEN Rules** | **Reference** | **Description** |
| 1  2  3 | **2021\_04\_15** | alert dns $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET PHISHING Observed Phish Domain in DNS Query (daviviendapersonalingresos .live) 2021-04-15"; dns.query; content:"daviviendapersonalingresos.live"; nocase; bsize:31; reference:url,twitter.com/TeamDreier/status/1382230430108254209; classtype:credential-theft; sid:2032763; rev:2; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_04\_15, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_04\_15;)  alert dns $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET EXPLOIT\_KIT Observed BottleEK Domain in DNS Lookup 2021-04-15"; dns.query; content:"ctgame.tk"; nocase; bsize:9; reference:url,twitter.com/nao\_sec/status/1381100024919035908; classtype:domain-c2; sid:2032764; rev:2; metadata:attack\_target Client\_Endpoint, created\_at 2021\_04\_15, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_04\_15;)  alert dns $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET PHISHING Observed Phish Domain in DNS Query (daviviendapersonalingresos .xyz) 2021-04-15"; dns.query; content:"daviviendapersonalingresos.xyz"; nocase; bsize:30; reference:url,twitter.com/TeamDreier/status/1382230430108254209; classtype:credential-theft; sid:2032765; rev:1; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_04\_15, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_04\_15;) | <https://twitter.com/TeamDreier/status/1382230430108254209>  <https://twitter.com/nao_sec/status/1381100024919035908>  <https://twitter.com/TeamDreier/status/1382230430108254209> | Fresh Bank Fraud from NS /dnspod.com observed. The following rules indicates the Exploit\_kit and Phishing domains  Involved in malicious activity.  [Emerging-Sigs] Ruleset Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-April/030293.html> |
| **4** | **2021\_04\_19** | alert tls $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET MALWARE Observed Win32/Wacapew.A!ml Domain in TLS SNI (zytrox .tk)"; flow:established,to\_server; tls.sni; content:"zytrox.tk"; bsize:9; classtype:domain-c2; sid:2032778; rev:1; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, created\_at 2021\_04\_19, deployment Perimeter, former\_category MALWARE, signature\_severity Major, updated\_at 2021\_04\_19;) |  | Observed a malicious remote code execution vulnerability on April 15th 2021 for this domain (zytrox[.]tk).  [Emerging-Sigs] Ruleset Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-April/030297.html>  Twitter Link:  <https://twitter.com/ET_Labs/status/1384280596025798658> |
| **5**  **6**  **7**  **8**  **9**  **10** | **2021\_04\_21** | alert dns $HOME\_NET any -> any any (msg:"ET INFO Observed DNS Query to DDNS Domain .myfirewall .org"; dns.query; content:".myfirewall.org"; endswith; fast\_pattern; classtype:bad-unknown; sid:2032792; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_04\_21, deployment Perimeter, former\_category INFO, signature\_severity Informational, updated\_at 2021\_04\_21;)  alert dns $HOME\_NET any -> any any (msg:"ET PHISHING Observed DNS Query to Phishing Domain (apiujpnkbrhsdn57oi0ns0qmbaj0wcdzjhblj6frlh1tr .eur .lc) "; dns.query; content:"apiujpnkbrhsdn57oi0ns0qmbaj0wcdzjhblj6frlh1tr.eur.lc"; bsize:52; fast\_pattern; classtype:domain-c2; sid:2032795; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_04\_21, deployment Perimeter, former\_category PHISHING, signature\_severity Minor, updated\_at 2021\_04\_21;)  alert dns $HOME\_NET any -> any any (msg:"ET PHISHING Observed DNS Query to Phishing Domain (hombreymaquina .com) "; dns.query; content:"hombreymaquina.com"; bsize:18; fast\_pattern; classtype:domain-c2; sid:2032796; rev:1; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_04\_21, deployment Perimeter, former\_category PHISHING, signature\_severity Minor, updated\_at 2021\_04\_21;)  alert dns $HOME\_NET any -> any any (msg:"ET PHISHING Observed DNS Query to Phishing Domain (igconsulting. pe) "; dns.query; content:"igconsulting.pe"; bsize:15; fast\_pattern; classtype:domain-c2; sid:2032797; rev:2; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, created\_at 2021\_04\_21, deployment Perimeter, former\_category PHISHING, signature\_severity Minor, updated\_at 2021\_04\_21;)  alert dns $HOME\_NET any -> any any (msg:"ET MALWARE Observed DNS Query to Ursnif CnC Domain (vorulenuke. us) "; dns.query; content:"vorulenuke.us"; bsize:13; fast\_pattern; classtype:domain-c2; sid:2032798; rev:1; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, created\_at 2021\_04\_21, deployment Perimeter, former\_category MALWARE, malware\_family ursnif, signature\_severity Major, updated\_at 2021\_04\_21;)  alert dns $HOME\_NET any -> any any (msg:"ET MALWARE Observed DNS Query to Ursnif CnC Domain (horulenuke .us) "; dns.query; content:"horulenuke.us"; bsize:13; fast\_pattern; classtype:domain-c2; sid:2032799; rev:1; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, created\_at 2021\_04\_21, deployment Perimeter, former\_category MALWARE, malware\_family ursnif, signature\_severity Major, updated\_at 2021\_04\_21;) |  | Following are some rules for ET INFO, ET MALWARE and ET PHISHING categories. Observed malicious domains involved in malicious activity over the internet.  [Emerging-Sigs] Ruleset Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-April/030301.html>  Twitter Link:  <https://twitter.com/ET_Labs/status/1385003961703309317> |
| **11**  **12**  **13** | **2021\_05\_06** | alert dns $HOME\_NET any -> any any (msg:"ET MALWARE Kimsuky APT CnC Domain in DNS Lookup"; dns.query; content:"download.riseknite.life"; bsize:23; nocase; reference:url,mp.weixin.qq.com/s/8RgFvA\_rOR2nIGxjWbEq-w; classtype:domain-c2; sid:2032920; rev:1; metadata:affected\_product Android, attack\_target Client\_Endpoint, created\_at 2021\_05\_06, deployment Perimeter, former\_category MALWARE, signature\_severity Major, updated\_at 2021\_05\_06;)  alert dns $HOME\_NET any -> any any (msg:"ET MALWARE Kimsuky APT CnC Domain in DNS Lookup"; dns.query; content:"onedrive-upload.ikpoo.cf"; bsize:24; nocase; reference:url,mp.weixin.qq.com/s/8RgFvA\_rOR2nIGxjWbEq-w; classtype:domain-c2; sid:2032921; rev:1; metadata:affected\_product Android, attack\_target Client\_Endpoint, created\_at 2021\_05\_06, deployment Perimeter, former\_category MALWARE, signature\_severity Major, updated\_at 2021\_05\_06;)  alert dns $HOME\_NET any -> any any (msg:"ET MALWARE Kimsuky APT CnC Domain in DNS Lookup"; dns.query; content:"alps.travelmountain.ml"; bsize:22; nocase; reference:url,mp.weixin.qq.com/s/8RgFvA\_rOR2nIGxjWbEq-w; classtype:domain-c2; sid:2032922; rev:1; metadata:affected\_product Android, attack\_target Client\_Endpoint, created\_at 2021\_05\_06, deployment Perimeter, former\_category MALWARE, signature\_severity Major, updated\_at 2021\_05\_06;) | <https://mp.weixin.qq.com/s/8RgFvA_rOR2nIGxjWbEq-w> | Following are some rules for ET MALWARE. Kimsuky APT Command and Control Domains are Observed in DNS Lookup.  [Emerging-Sigs] Ruleset Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-May/030317.html> |
| **14** | **2021\_05\_19** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Possible Phishing Landing Page 2021-05-18"; flow:established,from\_server; http.header; content:"|0d 0a|Content-Type|3a 20|text/html"; file.data; content:"<html>"; startswith; content:"<title>Mail Verification</title><script src=|27|http|3a 2f 2f|"; content:!"google."; within:20; content:"/google\_analytics\_auto.js|27|></script>"; distance:0; within:100; content:"<form method=|22|post|22 20|action=|22|x3d.php|22|"; distance:0; fast\_pattern; reference:url,app.any.run/tasks/654f09ca-352f-4d7a-a8eb-ce49c88b4f58/; classtype:credential-theft; sid:2033001; rev:1; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_05\_19, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_05\_19;) | <https://app.any.run/tasks/654f09ca-352f-4d7a-a8eb-ce49c88b4f58/> | This Rule is for ET PHISHING category and is written for a possible phishing landing page.  [Emerging-Sigs] Ruleset Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-May/030335.html>  Twitter link:  <https://twitter.com/ET_Labs/status/1395145739592929282> |
| **15** | **2021\_05\_28** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Possible Phishing Landing Page 2021-05-24"; flow:established,from\_server; http.header; content:"|0d 0a|Content-Type|3a 20|text/html"; file.data; content:"2|0a|<html>"; startswith; content:"<title>|26 23|47700|3b 26 23|51068|3b 20 26 23|49444|3b 26 23|51221|3b 20 7c 20 26 23|51060|3b 26 23|47700|3b 26 23|51068|3b 20 26 23|50629|3b 26 23|44536|3b 26 23|47112|3b 26 23|51060|3b 26 23|46300|3b|</title><script src=|27|/google\_analytics\_auto.js|27|></script>"; distance:0; fast\_pattern; content:"<form method=|22|post|22 20|action=|22|post.php|22|"; distance:0; reference:url,app.any.run/tasks/e878cb4f-4078-47c8-ac7c-59266940a68e/; classtype:social-engineering; sid:2033048; rev:1; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_05\_28, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_05\_28;) | <https://app.any.run/tasks/e878cb4f-4078-47c8-ac7c-59266940a68e/> | This Rules is for ET PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-May/030342.html>  Twitter Link:  <https://twitter.com/ET_Labs/status/1398405762507067395> |
| **16** | **2021\_06\_02** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed UK Gov Support Landing 2021-06-01"; flow:established,from\_server; file.data; content: "<title> Enter your Self Assessment Unique Taxpayer Reference|20 2d 20|Self|2d|Employment Income Support Scheme|20 2d 20|GOV.UK</title>"; fast\_pattern; content:"width=device-width"; distance:0; content:"initial-scale=1"; distance:0; content:"viewport-fit=cover|22 3e|"; reference:url,app.any.run/tasks/b1fe8d30-2f22-4f84-bcc8-2643562a8765/; classtype:social-engineering; sid:2033062; rev:1; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_06\_01, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_06\_01;) | <https://app.any.run/tasks/b1fe8d30-2f22-4f84-bcc8-2643562a8765/> | This rule belongs to PHISHING social-engineering category. A phishing landing page of UK Government Support is observed on 2021-06-01.  [Emerging-Sigs] Update Rules Summary Link:  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-June/030348.html>  Twitter Link:  <https://twitter.com/ET_Labs/status/1399851080620589059> |
| **17** | **2021-06-22** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed Possible Phishing Landing Page 2021-06-22"; flow:established,to\_client; file.data; content:"<title>L|26 23|79|3b|G|20 26 23|73|3b 26 23|78|3b 20|</title>"; fast\_pattern; content:"action=need1.php"; distance:0; content:"name=pfw"; distance:0; content:"method|3d|post|3e|"; distance:0 ; reference:url,app.any.run/tasks/fe8b5eb1-7aab-435f-9795-456983adc07e/; classtype:social-engineering; sid:2033155; rev:1; metadata:affected\_product Any, attack\_target Client\_Endpoint, created\_at 2021\_06\_22, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_06\_22;) | <https://app.any.run/tasks/fe8b5eb1-7aab-435f-9795-456983adc07e/> | [Emerging-Sigs] Update Summary Links:  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20210622>  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-June/030370.html> |
| **18** | **2021-06-25** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed Possible Phishing Landing Page 2021-06-24"; flow:established,to\_client; file.data; content:"<title>Red Link - BANCO DE LA NACION ARGENTINA</title>"; fast\_pattern; content:"enctype|3d 22|multipart|2f|form|2d|data|22 20|"; distance:0; content:"id|3d 22|UserNameVerificationForm|22|"; distance:0; content:"name|3d 22|UserNameVerificationForm|22|"; distance:0; content:"method|3d 22|post|22|"; distance:0; content:"action|3d 22|doLoginFirstStep.htm|22 3e|"; distance:0; reference:url,app.any.run/tasks/7ff1092c-4c9e-4915-933a-1f568b5ba83d; classtype:social-engineering; sid:2033187; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_06\_25, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_06\_25;) | <https://app.any.run/tasks/7ff1092c-4c9e-4915-933a-1f568b5ba83d> | [Emerging Sigs] Daily Ruleset update summary  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20210625>  <http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-June/030376.html> |
| **19**  **20** | **2021-07-01** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed Possible Phishing 2021-06-29"; flow:established,from\_server; file.data; content:"Webmail Login"; fast\_pattern; content:"action|3d 22|process.php|22|"; distance:0; content:"method|3d 22|post|22|"; distance:0; content:"target|3d 22 5f|top|22|"; distance:0; content:"style|3d 22|visibility|3a 22|>"; distance:0; reference:url,app.any.run/tasks/5fcdc0a0-7a79-4bcb-b2fb-3d358571d858/ ; classtype:social-engineering; sid:2033218; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_01, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_07\_01;)  alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed Possible Phishing Landing Page 2021-06-25"; flow:established,from\_server; file.data; content:"<title>Sign In</title>"; content:"role|3d 22|form|22|"; distance:0; content:"action|3d 22|squ.php|22|"; distance:0; content:"method|3d 22|post|22 3e|"; reference:url,app.any.run/tasks/a0625793-31c1-4538-a5c6-e213eb4b8128/; classtype:credential-theft; sid:2033215; rev:2; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_01, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_07\_01;) | <https://app.any.run/tasks/5fcdc0a0-7a79-4bcb-b2fb-3d358571d858/>  <https://app.any.run/tasks/a0625793-31c1-4538-a5c6-e213eb4b8128/> | [Emerging Sigs] Daily update ruleset summary link  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20210701>  Twitter Link:  <https://twitter.com/ET_Labs/status/1410728163995389956> |
| **21**  **22**  **23**  **24**  **25** | **2021-07-16** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M1"; flow:established,to\_server; http.method; content:"GET"; http.uri; content:"/if.cgi?redirect=setting.htm"; content:"TF\_submask=|22 3e 3c|script|3e|alert|28|"; fast\_pattern; content:"|29 3c 2f|script|3e|"; distance:0; reference:cve,2021-31250; reference:url,packetstormsecurity.com/files/162887/CHIYU-IoT-Cross-Site-Scripting.html; classtype:web-application-attack; sid:2033349; rev:2; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_16, cve CVE\_2021\_31250, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_07\_16;)  alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M2"; flow:established,to\_server; http.method; content:"GET"; http.uri; content:"/dhcp.cgi?redirect=setting.htm"; content:"TF\_hostname=|2f 22 3e 3c|img|20|src|3d 22 23 22 3e|"; fast\_pattern; reference:cve,2021-31250; reference:url,packetstormsecurity.com/files/162887/CHIYU-IoT-Cross-Site-Scripting.html; classtype:web-application-attack; sid:2033350; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_16, cve CVE\_2021\_31250, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_07\_16;)  alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M3"; flow:established,to\_server; http.method; content:"GET"; http.uri; content:"/ppp.cgi?redirect=setting.htm"; content:"TF\_servicename=|22 3e 3c|script|3e|alert|28|"; fast\_pattern; content:"|29 3c 2f|script|3e|"; distance:0; reference:cve,2021-31250; reference:url,packetstormsecurity.com/files/162887/CHIYU-IoT-Cross-Site-Scripting.html; classtype:web-application-attack; sid:2033351; rev:2; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_16, cve CVE\_2021\_31250, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_07\_16;)  alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M4"; flow:established,to\_server; http.method; content:"GET"; http.uri; content:"/man.cgi?redirect=setting.htm"; content:"TF\_port=|2f 22 3e 3c|img|20|src|3d 22 23 22 3e|"; fast\_pattern; reference:cve,2021-31250; reference:url,packetstormsecurity.com/files/162887/CHIYU-IoT-Cross-Site-Scripting.html; classtype:web-application-attack; sid:2033352; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_16, cve CVE\_2021\_31250, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_07\_16;)  alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET EXPLOIT Stored XSS and Webpass IoT devices CVE-2021-31643"; flow:established,to\_server; http.method; content:"GET"; http.uri; content:"/if.cgi?redirect=EmpRcd.htm"; content:"&username=|22 3e 3c|script|3e|alert|28|"; fast\_pattern; content:"|29 3c 2f|script|3c|"; distance:0; reference:cve,2021-31643; reference:url,packetstormsecurity.com/files/162887/CHIYU-IoT-Cross-Site-Scripting.html; classtype:web-application-attack; sid:2033353; rev:2; metadata:attack\_target Client\_Endpoint, created\_at 2021\_07\_16, cve CVE\_2021\_31643, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_07\_16;) | <https://packetstormsecurity.com/files/162887/CHIYU-IoT-Cross-Site-Scripting.html> | [Emerging Sigs] Latest Update Ruleset Summary Link:  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20210716>  Twitter Link:  <https://twitter.com/ET_Labs/status/1416164287815557127> |
| **26** | **2021-07-19** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET EXPLOIT CHIYU IoT Devices - Denial of Service"; flow:established,to\_server; http.method; content:"GET"; http.uri; content:"/if.cgi?redirect=AccLog.htm"; startswith; content:"&type=go\_log\_page&page=2781000"; endswith; fast\_pattern; http.referer; content:"/AccLog.htm"; endswith; reference:cve,2021-31642; reference:url,www.exploit-db.com/exploits/49937; classtype:denial-of-service; sid:2033362; rev:2; metadata:affected\_product IoT, attack\_target Client\_Endpoint, created\_at 2021\_07\_19, deployment Perimeter, former\_category EXPLOIT, signature\_severity Major, updated\_at 2021\_07\_19;) | [www.exploit-db.com/exploits/49937](http://www.exploit-db.com/exploits/49937)  cve-2021-31642 | [Emerging-Sig] Daily Update ruleset summary Link  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20210719> |
| **27**  **28** | **2021-08-09** | alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed OneDrive Phishing Landing Page 2021-08-09"; flow:established,from\_server; file.data; content:"<title>|0d 0a 09|Files - OneDrive|0d 0a|</title>"; fast\_pattern; content:"<form method|3d 22|post|22|"; distance:0; content:"action|3d 22|link.php|22|"; distance:0; reference:url,app.any.run/tasks/7d82fceb-ac0f-452a-9b37-4c87478f2df6; classtype:social-engineering; sid:2033696; rev:1; metadata:attack\_target Client\_Endpoint, created\_at 2021\_08\_09, deployment Perimeter, former\_category PHISHING, signature\_severity Major, updated\_at 2021\_08\_09;)  alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET PHISHING Observed Zimbra Phishing Landing Page 2021-08-09"; flow:established,from\_server; file.data; content:"<title>Zimbra Web Client Sign In</title>"; content:"<form method|3d 22|post|22|"; distance:0; content:"name|3d 22|loginForm|22|"; distance:0; content:"action|3d 22|mll.php|22|"; distance:0; fast\_pattern; content:"accept-charset|3d 22|UTF-8|22|"; reference:url,app.any.run/tasks/bda22930-0bfb-4ccd-b5c4-26f526b8cba7; classtype:social-engineering; sid:2033697; rev:1; metadata:created\_at 2021\_08\_09, former\_category PHISHING, updated\_at 2021\_08\_09;) | <https://app.any.run/tasks/7d82fceb-ac0f-452a-9b37-4c87478f2df6>  <https://app.any.run/tasks/bda22930-0bfb-4ccd-b5c4-26f526b8cba7> | [Emerging-Sigs] Update Ruleset summary link  <https://lists.emergingthreats.net/pipermail/emerging-sigs/2021-August/030416.html>  Twitter Link:  <https://twitter.com/ET_Labs/status/1424861793986433030> |
| **29**  **30**  **31**  **32**  **33** | **2021-08-30** | alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT Realtek SDK - Command Injection Inbound (CVE-2021-35395)"; flow:established,to\_server; http.method; content:"POST"; http.uri; content:"/goform/formWsc"; fast\_pattern; endswith; http.request\_body; content:"peerPin="; content:"|3b|"; distance:0; within:50; reference:url,www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/; reference:cve,2021-35395; classtype:attempted-user; sid:2033840; rev:2; metadata:attack\_target Server, created\_at 2021\_08\_30, cve CVE\_2021\_35395, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_08\_30;)   alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT Possible Realtek SDK - formStaticDHCP Stack Buffer Overflow Inbound (CVE-2021-35393)"; flow:established,to\_server; http.method; content:"POST"; http.uri; content:"/goform/formStaticDHCP"; endswith; fast\_pattern; http.request\_body; content:"hostname="; pcre:"/^[^&]{42,}/"; reference:url,www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/; reference:cve,2021-35393; classtype:attempted-user; sid:2033841; rev:1; metadata:attack\_target Server, created\_at 2021\_08\_30, cve CVE\_2021\_35393, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_08\_30;)   alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT Possible Realtek SDK - formWlanMultipleAP Stack Buffer Overflow Inbound (CVE-2021-35393)"; flow:established,to\_server; http.method; content:"POST"; http.uri; content:"/goform/formWlanMultipleAP"; endswith; fast\_pattern; http.request\_body; content:"submit-url="; pcre:"/^[^&]{512,}/"; reference:url,www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/; reference:cve,2021-35393; classtype:attempted-user; sid:2033842; rev:1; metadata:attack\_target Server, created\_at 2021\_08\_30, cve CVE\_2021\_35393, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_08\_30;)   alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT Possible Realtek SDK - formRebootCheck/formWsc Stack Buffer Overflow Inbound (CVE-2021-35392)"; flow:established,to\_server; http.method; content:"POST"; http.uri; content:"/goform/"; pcre:"/^form(RebootCheck|Wsc)$/R"; http.request\_body; content:"submit-url="; fast\_pattern; isdataat:2000,relative; reference:url,www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/; reference:cve,2021-35392; classtype:attempted-user; sid:2033837; rev:1; metadata:attack\_target Server, created\_at 2021\_08\_30, cve CVE\_2021\_35392, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_08\_30;)   alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT Possible Realtek SDK - formWlSiteSurvey Stack Buffer Overflow Inbound (CVE-2021-35393)"; flow:established,to\_server; http.method; content:"POST"; http.uri; content:"/goform/formWlSiteSurvey"; fast\_pattern; endswith; http.request\_body; content:"ifname="; pcre:"/^[^&]{90,}/"; reference:url,www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/; reference:cve,2021-35393; classtype:attempted-user; sid:2033838; rev:2; metadata:attack\_target Server, created\_at 2021\_08\_30, cve CVE\_2021\_35393, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_08\_30;) | <https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/>  CVE\_2021\_35395  CVE-2021-35392 | Multiple rules on Realtek SDK IoT supply chain vulnerabilities including command injection and stack buffer overflow vulnerabilities.  [Emerging-Sigs] Daily update ruleset summary link:  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20210830>  Twitter Link:  <https://twitter.com/ET_Labs/status/1432466603174731777> |
| **34 35** | **2021-10-11** | alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT RUIJIE NBR/RGNBR Command Injection Attempt Inbound M1"; flow:established,to\_server; http.uri; content:"/wget\_test.asp?"; fast\_pattern; content:"="; distance:0; within:5; pcre:"/^(?:\x3b|\x0a|\x26|\x60|\x7C|\x24)/R"; classtype:attempted-admin; sid:2034161; rev:1; metadata:attack\_target Networking\_Equipment, created\_at 2021\_10\_09, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_10\_09;)  alert http any any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT RUIJIE NBR/RGNBR Command Injection Attempt Inbound M2"; flow:established,to\_server; http.uri; content:"/wget\_test.asp?"; fast\_pattern; http.uri.raw; content:"="; pcre:"/^%(?:3b|0a|26|60|7C|24)/R"; classtype:attempted-admin; sid:2034162; rev:1; metadata:attack\_target Networking\_Equipment, created\_at 2021\_10\_09, deployment Perimeter, deployment Internal, former\_category EXPLOIT, signature\_severity Major, tag Exploit, updated\_at 2021\_10\_09;) | <https://blog.netlab.360.com/rimasuta-spread-with-ruijie-0day-en/?&web_view=true> | Daily Update Ruleset Summary Link:  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20211011> |
| **36** | **2021\_11\_09** | alert http $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET MALWARE RedLine - GetArguments Request"; flow:established,to\_server; http.method; content:"POST"; http.header; content:"|0d 0a|SOAPAction|3a 20 22|http://tempuri.org/"; http.request\_body; content:"|3c 73 3a|Body|3e 3c|GetArguments|20|xmlns=|22|http|3a 2f 2f|tempuri|2e|org|2f 22 2f|"; fast\_pattern; reference:md5,9a3ac9f18c1222e7a77a47db01b1f597; classtype:command-and-control; sid:2034361; rev:1; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, created\_at 2021\_04\_14, deployment Perimeter, former\_category MALWARE, malware\_family Redline, signature\_severity Major, updated\_at 2021\_04\_14;) | <https://app.any.run/tasks/194b6f7b-8ce1-4052-98a0-18cf27fd6e56/> | Daily Ruleset update summary  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20211109>  Twitter:  <https://twitter.com/ET_Labs/status/1458217894521753604> |
| **37** | **2022\_04\_15** | alert http $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET PHISHING Successful Wells Fargo Phish 2021-03-16"; flow:established,to\_server; http.method; content:"POST"; http.request\_body; content:"j\_username="; depth:11; nocase; content:"&j\_password="; nocase; distance:0; content:"&save-username="; nocase; distance:0; content:"&hdnuserid="; nocase; distance:0; content:"&btnSignon=Sign+On&screenid=SIGNON&origination="; nocase; distance:0; fast\_pattern; classtype:credential-theft; sid:2036221; rev:2; metadata:affected\_product Web\_Browsers, attack\_target Client\_Endpoint, created\_at 2021\_03\_16, deployment Perimeter, former\_category PHISHING, signature\_severity Critical, tag Phishing, updated\_at 2021\_03\_16, mitre\_tactic\_id TA0001, mitre\_tactic\_name Initial\_Access, mitre\_technique\_id T1566, mitre\_technique\_name Phishing;) |  | Daily Ruleset summary Link:  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20220415> |
| **38**  **39** | **2022\_04\_16** | alert http any any -> $HOME\_NET any (msg:"ET WEB\_SERVER Possible Oracle SQL Injection utl\_inaddr call in URI"; flow:established,to\_server; http.uri; content:"utl\_inaddr.get\_host"; nocase; fast\_pattern; classtype:attempted-admin; sid:2015749; rev:5; metadata:affected\_product Web\_Server\_Applications, attack\_target Web\_Server, created\_at 2012\_09\_28, deployment Datacenter, signature\_severity Major, tag SQL\_Injection, updated\_at 2022\_04\_18;)  alert http $EXTERNAL\_NET any -> [$HOME\_NET,$HTTP\_SERVERS] any (msg:"ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M2"; flow:established,to\_server; http.uri.raw; pcre:"/^\/(?:icons|cgi-bin)/"; content:"/.%2e/.%2e/.%2e/.%2e/"; reference:url,httpd.apache.org/security/vulnerabilities\_24.html; reference:url,github.com/iilegacyyii/PoC-CVE-2021-41773/blob/main/CVE-2021-41773.py; reference:cve,2021-41773; classtype:attempted-admin; sid:2034125; rev:4; metadata:affected\_product Apache\_HTTP\_server, attack\_target Web\_Server, created\_at 2021\_10\_05, cve CVE\_2021\_41773, deployment Perimeter, deployment Internet, former\_category EXPLOIT, performance\_impact Low, signature\_severity Major, updated\_at 2022\_04\_18;) |  | Daily Ruleset update summary Link:  <https://www.proofpoint.com/us/daily-ruleset-update-summary-20220418> |
|  |  |  |  |  |
|  |  |  |  |  |