## All below rules are available on <a href="https://rules.emergingthreats.net/open/suricata-5.0/emerging-all.rules">https://rules.emergingthreats.net/open/suricata-5.0/emerging-all.rules</a>

Sr. No	Date	ET OPEN Rules	Reference	Description
1 2 3	2021_0 4_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;)	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:
		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/st atus/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;)	https://twitter.com /nao_sec/status/13 811000249190359 08	http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- April/030293.html
		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,	https://twitter.com /TeamDreier/statu s/13822304301082 54209	

		<pre>signature_severity Major, updated_at 2021_04_15;)</pre>	
4	2021_0 4_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 15 <sup>th</sup> 2021 for this domain (zytrox[.]tk). [Emerging-Sigs] Ruleset Summary Link:  http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- April/030297.html  Twitter Link: https://twitter.com /ET_Labs/status/13 842805960257986 58
5 6 7 8 9 10	2021_0 4_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 (apiujpnkbrhsdn57oi0ns0qmbaj0wcdzjhb lj6frlh1tr .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,	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:

former category PHISHING, https://twitter.com signature severity Minor, updated at /ET Labs/status/13 2021 04 21;) 850039617033093 17 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  $\overline{7}$  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

		T 1 =	T	<del>                                     </del>
		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;)		
11	2021 0	alert dns \$HOME NET any -> any any	https://mp.wei	Following are some
12	5_06	(msg:"ET MALWARE Kimsuky APT CnC	xin.qq.com/s/8	rules for ET
13	<b>-</b>	Domain in DNS Lookup"; dns.query;	RgFvA_rOR2nIGx	MALWARE.
		<pre>content:"download.riseknite.life"; bsize:23; nocase;</pre>	<u>jWbEq-w</u>	Kimsuky APT
		reference:url,mp.weixin.qq.com/s/8Rg		Command and
		FvA rOR2nIGxjWbEq-w;		Control Domains
		classtype:domain-c2; sid:2032920;		are Observed in
		rev:1; metadata:affected_product		DNS Lookup.
		Android, attack_target		•
		Client_Endpoint, created_at 2021 05 06, deployment Perimeter,		[Emerging-Sigs]
		former category MALWARE,		Ruleset Summary
		signature_severity Major, updated_at		Link:
		2021_05_06;)		
		alert dns \$HOME NET any -> any any		http://lists.emergin
		(msg:"ET MALWARE Kimsuky APT CnC		gthreats.net/piper
		Domain in DNS Lookup"; dns.query;		mail/emerging-
		<pre>content:"onedrive-upload.ikpoo.cf";</pre>		sigs/2021-
		bsize:24; nocase;		May/030317.html
		<pre>reference:url,mp.weixin.qq.com/s/8Rg FvA rOR2nIGxjWbEq-w;</pre>		
		classtype:domain-c2; sid:2032921;		
		rev:1; metadata:affected product		
		Android, attack_target		
		Client_Endpoint, created_at		
		2021_05_06, deployment Perimeter,		
		<pre>former_category MALWARE, signature severity Major, updated at</pre>		
		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/8Rg		
		<pre>FvA_rOR2nIGxjWbEq-w;</pre>		
		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;)		

	1			
14	2021_0	alert http \$EXTERNAL_NET any ->	https://app.an	This Rule is for ET
	5_19	\$HOME NET any (msg:"ET PHISHING	y.run/tasks/65	PHISHING category
		Possible Phishing Landing Page 2021-	4f09ca-352f-	and is written for a
		05-18";	4d7a-a8eb-	possible phishing
		flow:established, from_server;	<u>ce49c88b4f58/</u>	
		http.header; content:" 0d		landing page.
		<pre>0a Content-Type 3a 20 text/html";</pre>		
		<pre>file.data; content:"<html>";</html></pre>		[Emerging-Sigs]
		startswith; content:" <title>Mail&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;Ruleset Summary&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;Verification</title> <script< th=""><th></th><th>Link:</th></script<>		Link:
		src= 27 http 3a 2f 2f ";		http://lists.emergin
		content:!"google."; within:20;		
		content:"/google_analytics_auto.js 2		gthreats.net/piper
		7 >"; distance:0; within:100; content:" <form< th=""><th></th><th>mail/emerging-</th></form<>		mail/emerging-
		method= 22 post 22		sigs/2021-
		20 action= 22 x3d.php 22 ";		May/030335.html
		distance:0; fast pattern;		
		reference:url,app.any.run/tasks/654f		Twitter link:
		09ca-352f-4d7a-a8eb-ce49c88b4f58/;		
		classtype:credential-theft;		https://twitter.com
		sid:2033001; rev:1;		/ET_Labs/status/13
		metadata:affected product Any,		<u>951457395929292</u>
		attack target Client Endpoint,		<u>82</u>
		created at 2021 05 19, deployment		
		Perimeter, former category PHISHING,		
		signature severity Major, updated at		
		2021 05 19;)		
15	2021 0	alert http \$EXTERNAL NET any ->		This Rules is for FT
15	2021_0	\$HOME_NET any (msg:"ET PHISHING	https://app.an	This Rules is for ET
15	2021_0 5_28		https://app.an y.run/tasks/e8	PHISHING category
15	_	\$HOME_NET any (msg:"ET PHISHING Possible Phishing Landing Page 2021-05-24";	https://app.an y.run/tasks/e8 78cb4f-4078-	PHISHING category and is written for a
15	_	\$HOME_NET any (msg:"ET PHISHING Possible Phishing Landing Page 2021- 05-24"; flow:established, from_server;	<pre>y.run/tasks/e8</pre>	PHISHING category and is written for a phishing landing
15	_	\$HOME_NET any (msg:"ET PHISHING Possible Phishing Landing Page 2021- 05-24"; flow:established, from_server; http.header; content:" 0d	y.run/tasks/e8 78cb4f-4078-	PHISHING category and is written for a
15	_	\$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";	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing
15	_	\$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>";</html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing
15	_	\$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&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category&lt;br&gt;and is written for a&lt;br&gt;phishing landing&lt;br&gt;page.&lt;br&gt;[Emerging-Sigs]&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 26 23 47700 3b 26 23 51068 3b 20 26&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category&lt;br&gt;and is written for a&lt;br&gt;phishing landing&lt;br&gt;page.&lt;br&gt;[Emerging-Sigs]&lt;br&gt;Ruleset Update&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 26 23 47700 3b 26 23 51068 3b 20 26 23 49444 3b 26 23 51221 3b 20 7c 20&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category&lt;br&gt;and is written for a&lt;br&gt;phishing landing&lt;br&gt;page.&lt;br&gt;[Emerging-Sigs]&lt;br&gt;Ruleset Update&lt;br&gt;Summary Link:&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 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&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 26 23 47700 3b 26 23 51068 3b 20 26 23 49444 3b 26 23 51221 3b 20 7c 20 26 23 51068 3b 20 26 23 50629 3b 26&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergingthreats.net/piper&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 26 23 47700 3b 26 23 51068 3b 20 26 23 49444 3b 26 23 51221 3b 20 7c 20 26 23 51068 3b 20 26 23 47700 3b 26 23 51068 3b 20 26 23 50629 3b 26 23 44536 3b 26 23 47112 3b 26&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 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&lt;/th&gt;&lt;th&gt;y.run/tasks/e8&lt;br&gt;78cb4f-4078-&lt;br&gt;47c8-ac7c-&lt;/th&gt;&lt;th&gt;PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergingthreats.net/piper&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;15&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;\$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 &lt;html&gt;"; startswith; content:"&lt;title&gt; 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< th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-</th></script<></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergingthreats.net/pipermail/emerging-sigs/2021-
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27&lt;/th"><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergingthreats.net/pipermail/emerging-</th></tr><tr><th>15</th><th>_</th><th>\$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 47700 3b 26 23 51060 3b 26 23 46300 3b </title><script src= 27 /google_analytics_auto.js 27  ></script>"; distance:0;</html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	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
15	_	\$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 47700 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< th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link:</th></form<></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link:
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form method=" 22 post 22&lt;/th"><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>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</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	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
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form 20 action=' 22 post.php 22 ";&lt;/th' method=" 22 post 22"><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13
15	_	\$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 51221 3b 20 7c 20 26 23 51068 3b 20 26 23 50629 3b 26 23 44536 3b 26 23 47712 3b 26 23 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form 20 action=' 22 post.php 22 ";' distance:0;<="" method=" 22 post 22" th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>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</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	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
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form 20 action=' 22 post.php 22 ";' distance:0;="" e878<="" method=" 22 post 22" reference:url,app.any.run="" tasks="" th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form 20 action=' 22 post.php 22 ";' ;<="" cb4f-4078-47c8-ac7c-59266940a68e="" distance:0;="" e878="" method=" 22 post 22" reference:url,app.any.run="" tasks="" th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form 20 action=' 22 post.php 22 ";' distance:0;="" e878<="" method=" 22 post 22" reference:url,app.any.run="" tasks="" th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673
15	_	\$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 46300 3b </title><script src=" 27 /google_analytics_auto.js 27"  =""></script>"; distance:0; fast_pattern; content:"<form 20 action=' 22 post.php 22 ";' ;="" cb4f-4078-47c8-ac7c-59266940a68e="" classtype:social-engineering;<="" distance:0;="" e878="" method=" 22 post 22" reference:url,app.any.run="" tasks="" th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673
15	_	\$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 20 action=' 22 post.php 22 ";' ;="" cb4f-4078-47c8-ac7c-59266940a68e="" classtype:social-engineering;="" distance:0;="" e878="" method=" 22 post 22" reference:url,app.any.run="" rev:1;<="" sid:2033048;="" tasks="" th=""><th>y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-</th><th>PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673</th></form></html>	y.run/tasks/e8 78cb4f-4078- 47c8-ac7c-	PHISHING category and is written for a phishing landing page.  [Emerging-Sigs] Ruleset Update Summary Link: http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- May/030342.html  Twitter Link: https://twitter.com /ET_Labs/status/13 984057625070673

		anatad at 2021 05 20 damlarmant		
		created_at 2021_05_28, deployment Perimeter, former_category PHISHING, signature_severity Major, updated_at 2021_05_28;)		
16	2021_0 6_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/blfe 8d30-2f22-4f84-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.an y.run/tasks/b1 fe8d30-2f22- 4f84-bcc8- 2643562a8765/	This rule belongs to PHISHING socialengineering 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/139851080620589059
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/fe8b 5eb1-7aab-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,	https://app.any.run/tasks/fe8b 5eb1-7aab- 435f-9795- 456983adc07e/	[Emerging-Sigs] Update Summary Links: https://www.proof point.com/us/daily -ruleset-update- summary- 20210622 http://lists.emergin gthreats.net/piper mail/emerging- sigs/2021- June/030370.html

18	2021-	<pre>signature_severity Major, updated_at 2021_06_22;)  alert http \$EXTERNAL NET any -&gt;</pre>	https://app.an	[Emerging Sigs]
	06-25	SHOME_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 UserNameVerificationForm 22 "; distance:0; content:"method 3d 22 Jost 22 "; distance:0; content:"action 3d 22 doLoginFirstStep.htm 22 3e "; distance:0; reference:url,app.any.run/tasks/7ff1 092c-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;)	y.run/tasks/7f f1092c-4c9e- 4915-933a- 1f568b5ba83d	Daily Ruleset update summary https://www.proof point.com/us/daily -ruleset-update- summary- 20210625  http://lists.emergin gthreats.net/piper mail/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/5fcd c0a0-7a79-4bcb-b2fb-3d358571d858/; classtype:social-engineering; sid:2033218; rev:1; metadata:attack_target Client_Endpoint, created_at 2021_07_01, deployment Perimeter, former_category PHISHING,	https://app.an y.run/tasks/5f cdc0a0-7a79- 4bcb-b2fb- 3d358571d858/	[Emerging Sigs] Daily update ruleset summary link  https://www.proof point.com/us/daily -ruleset-update- summary- 20210701  Twitter Link: https://twitter.com /ET_Labs/status/14 107281639953899 56

		signature_severity Major, updated_at		
		2021_07_01;)		
		<pre>alert http \$EXTERNAL_NET any -&gt; \$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/a062 5793-31c1-4538-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;)</pre>	https://app.an y.run/tasks/a0 625793-31c1- 4538-a5c6- e213eb4b8128/	
21 22 23 24 25	2021- 07-16	<pre>alert http \$EXTERNAL_NET any -&gt; \$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.ht m"; 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.co m/files/162887/CHIYU-IoT-Cross-Site-</pre>	https://packet stormsecurity. com/files/1628 87/CHIYU-IOT- Cross-Site- Scripting.html	[Emerging Sigs] Latest Update Ruleset Summary Link: https://www.proof point.com/us/daily -ruleset-update- summary- 20210716  Twitter Link: https://twitter.com
		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-		/ET Labs/status/14 161642878155571 27
		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 | imq | 20 | src | 3d  22  23  22  3e | ";
fast pattern; reference:cve,2021-
31250;
reference:url,packetstormsecurity.co
m/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.h
tm"; 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.co
m/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.h
tm"; content:"TF port=|2f 22 3e
3c|img|20|src|3d 22 23 22 3e|";
fast pattern; reference:cve, 2021-
31250;
reference:url, packetstormsecurity.co
m/files/162887/CHIYU-IoT-Cross-Site-
```

	1		1	
		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.co m/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;)		
26	2021-	alert http \$EXTERNAL_NET any ->	www.exploit-	[Emerging-Sig]
	07-19	\$HOME_NET any (msg:"ET EXPLOIT CHIYU IoT Devices - Denial of Service";	db.com/exploit s/49937	Daily Update
		<pre>flow:established,to_server;</pre>		ruleset summary Link
		<pre>http.method; content:"GET"; http.uri;</pre>	cve-2021-31642	Lank
		content:"/if.cgi?redirect=AccLog.htm		https://www.proof
		"; startswith; content:"&type=go log page&page=2781		point.com/us/daily
		000"; endswith; fast_pattern;		<u>-ruleset-update-</u> summary-
		<pre>http.referer; content:"/AccLog.htm"; endswith; reference:cve,2021-31642;</pre>		<u>20210719</u>
		reference:url,www.exploit-		
		<pre>db.com/exploits/49937; classtype:denial-of-service;</pre>		
		sid:20333362; rev:2;		
		<pre>metadata:affected_product IoT, attack target Client Endpoint,</pre>		
		created_at 2021_07_19, deployment		
		Perimeter, former_category EXPLOIT, signature severity Major, updated at		
		2021_07_19;)		

27	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 2021_08_09,="" 2021_08_09;)<="" 22 link.php 22 ";="" 22 post 22 ";="" 7d82="" classtype:social-engineering;="" client_endpoint,="" content:"action 3d="" created_at="" deployment="" distance:0;="" fceb-ac0f-452a-9b37-4c87478f2df6;="" former_category="" major,="" metadata:attack_target="" method 3d="" perimeter,="" phishing,="" reference:url,app.any.run="" rev:1;="" sid:2033696;="" signature_severity="" tasks="" th="" updated_at=""><th>https://app.an y.run/tasks/7d 82fceb-ac0f- 452a-9b37- 4c87478f2df6</th><th>[Emerging-Sigs] Update Ruleset summary link  https://lists.emergi ngthreats.net/pipe rmail/emerging- sigs/2021- August/030416.ht ml  Twitter Link: https://twitter.com /ET_Labs/status/14 248617939864330 30</th></form>	https://app.an y.run/tasks/7d 82fceb-ac0f- 452a-9b37- 4c87478f2df6	[Emerging-Sigs] Update Ruleset summary link  https://lists.emergi ngthreats.net/pipe rmail/emerging- sigs/2021- August/030416.ht ml  Twitter Link: https://twitter.com /ET_Labs/status/14 248617939864330 30
28		<pre>alert http \$EXTERNAL_NET any -&gt; \$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 2021_08_09,="" 2021_08_09;)<="" 22 loginform 22 ";="" 22 mll.php 22 ";="" 22 post 22 ";="" 22 utf-8 22 ";="" 2930-0bfb-4ccd-b5c4-26f526b8cba7;="" bda2="" charset 3d="" classtype:social-engineering;="" content:"accept-="" content:"action 3d="" content:"name 3d="" distance:0;="" fast_pattern;="" former_category="" metadata:created_at="" method 3d="" phishing,="" pre="" reference:url,app.any.run="" rev:1;="" sid:2033697;="" tasks="" updated_at=""></form></pre>	https://app.an y.run/tasks/bd a22930-0bfb- 4ccd-b5c4- 26f526b8cba7	
29 30 31 32 33	2021- 08-30	<pre>alert http any any -&gt;   [\$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-</pre>	https://www.io t- inspector.com/ blog/advisory- multiple- issues- realtek-sdk- iot-supply- chain/  CVE_2021_35395	Multiple rules on Realtek SDK IoT supply chain vulnerabilities including command injection and stack buffer overflow vulnerabilities.

inspector.com/blog/advisorymultiple-issues-realtek-sdk-iotsupply-chain/; reference:cve,202135395; 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.iotinspector.com/blog/advisorymultiple-issues-realtek-sdk-iotsupply-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-202135393)"; flow:established,to\_server;
http.method; content:"POST";
http.uri;
content:"/goform/formWlanMultipleAP"
; endswith; fast\_pattern;
http.request\_body; content:"submiturl="; pcre:"/^[^&]{512,}/";
reference:url,www.iotinspector.com/blog/advisorymultiple-issues-realtek-sdk-iot-

CVE-2021-35392

Daily update ruleset summary link:

https://www.proof point.com/us/daily -ruleset-updatesummary-20210830

## Twitter Link:

https://twitter.com /ET\_Labs/status/14 324666031747317 77

```
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;
```

				T
		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;)		
34	2021-	alert http any any ->	https://blog.netlab.	Daily Update
35	10-11	[\$HOME NET,\$HTTP SERVERS] any		Ruleset Summary
33	10-11	(msg:"ET EXPLOIT RUIJIE NBR/RGNBR	360.com/rimasuta-	·
		Command Injection Attempt Inbound	spread-with-ruijie-	Link:
		M1"; flow:established,to server;	<u>Oday-</u>	
		http.uri; content:"/wget test.asp?";	en/?&web_view=tr	https://www.proof
		fast pattern; content:"=";	ue	point.com/us/daily
		distance:0; within:5;	_	-ruleset-update-
		pcre:"/^(?:\x3b \x0a \x26 \x60 \x7C		summary-
		\x24)/R"; classtype:attempted-admin;		20211011
		sid:2034161; rev:1;		20211011
		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;		
		<pre>http.uri; content:"/wget_test.asp?";</pre>		
		<pre>fast_pattern; http.uri.raw;</pre>		
		content:"=";		
		pcre:"/^%(?:3b 0a 26 60 7C 24)/R";		
		<pre>classtype:attempted-admin;</pre>		
		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;)		
36	2021_1	alert http \$HOME_NET any ->	https://app.a	Daily Ruleset
	1_09	\$EXTERNAL_NET any (msg:"ET MALWARE	<pre>ny.run/tasks/</pre>	update summary
	_	RedLine - GetArguments Request";	<u>194b6f7b-</u>	,
		flow:established, to_server;	8ce1-4052-	https://www.proof
		http.method; content:"POST";	<u>98a0-</u>	
		http.header; content:" 0d	18cf27fd6e56/	point.com/us/daily
		0a SOAPAction 3a 20		-ruleset-update-
		22 http://tempuri.org/";		summary-
		http.request_body; content:" 3c 73 3a Body 3e		<u>20211109</u>
		3c GetArguments 20 xmlns= 22 http 3a 2f 2f tempuri 2e org 2f 22 2f ";		
		zi zi tempuri ze org zi zz zi ";   fast pattern;		
		Tape_harrell,		

		reference:md5,9a3ac9f18c1222e7a77a47	Twitter:	
		db01b1f597; classtype:command-and-control; sid:2034361; rev:1;	https://twitter.	
		metadata:affected product	/ET_Labs/statu	ıs/14
		Windows XP Vista 7 8 10 Server 32 64	<u>582178945217</u>	<u> 536</u>
		Bit, attack target Client Endpoint,	04	
		created at 2021 04 14, deployment		
		Perimeter, former category MALWARE,		
		malware family Redline,		
		signature severity Major, updated at		
		2021 04 14;)		
37	2022 0	alert http \$HOME NET any ->	Daily Ruleset	
"	4_15	\$EXTERNAL NET any (msg:"ET PHISHING	summary Link:	
	4_13	Successful Wells Fargo Phish 2021-	Sullillary Link.	
		03-16"; flow:established,to_server;	1	
		http.method; content:"POST";	https://www.p	
		http.request_body;	point.com/us/o	daily
		<pre>content:"j_username="; depth:11;</pre>	-ruleset-update	<del>2-</del>
		<pre>nocase; content:"&amp;j_password=";</pre>	summary-	
		nocase; distance:0; content:"&save-	20220415	
		<pre>username="; nocase; distance:0;</pre>	20220413	
		<pre>content:"&amp;hdnuserid="; nocase;</pre>		
		distance:0;		
		content: "&btnSignon=Sign+On&screenid		
		=SIGNON&origination="; nocase;		
		<pre>distance:0; fast_pattern;</pre>		
		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;)		
38	2022_0	alert http any any -> \$HOME NET any	Daily Ruleset	
39	4_16	(msg:"ET WEB_SERVER Possible Oracle	update summa	ırv
33	4_10	SQL Injection utl_inaddr call in	Link:	ıı y
		<pre>URI"; flow:established,to_server;</pre>	Link:	
		http.uri;		
		<pre>content:"utl_inaddr.get_host";</pre>	https://www.p	
		nocase; fast_pattern;	point.com/us/d	daily
		<pre>classtype:attempted-admin;</pre>	-ruleset-update	e-
		sid:2015749; rev:5;	summary-	_
		metadata:affected_product	20220418	
		Web_Server_Applications,	20220418	
		attack_target Web_Server, created_at		
		2012_09_28, deployment Datacenter,		
		signature_severity Major, tag		
		SQL_Injection, updated_at		
		2022_04_18;)		

 T	Γ	
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/secur ity/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;)		