

SlashNext Phishing Protection

Phishing Protection Accuracy vs. Leading Email Security Providers

EXECUTIVE SUMMARY

Phishing attacks are not new but the sophistication of the attacks and, thus, their effectiveness is always growing. Instead of mass attacks many bad actors use targeted, "spear phishing" attacks. SlashNext has developed next-gen AI phishing threat intelligence and protection to help combat this omnipresent threat.

SlashNext commissioned Tolly to benchmark the accuracy of its phishing protection solution and compare that with several leading vendors of email security solutions. Tests were conducted with Microsoft Defender (Safe Links) and Proofpoint Essentials Business (URL Defense). An informal test was also run against the advanced threat protection offering, including their URL rewriting feature, from another market leading provider (Vendor X). The test corpus consisted of zero-hour phishing URLs submitted to the PhishTank community site as well as those discovered by SlashNext's Threat Labs.

SlashNext delivered significantly greater accuracy on the zero-hour PhishTank URLs than the other solutions. Significantly, the other solutions could only identify 21% to 49% of the recent and zero-hour phishing URLs selected by Tolly from the SlashNext AI Phishing Detection Database. See Figure 1.

THE BOTTOM LINE

SlashNext Phishing Protection:

- 1 Delivered the highest spear phishing detection rate at 98.1%
- 2 Provides threat intelligence scope beyond that of other solutions tested. Other solutions blocked between 21.3%-49.3% of the phishing URLs from SlashNext AI Phishing Detection Database
- 3 Provides URL protection against email and non-email borne threats
- 4 Easily implemented as a browser extension in minutes

URL Phishing Detection Accuracy

	ALL URLs	PhishTank URLs	SlashNext URLs
SlashNext SlashNext Browser Protection	98.1%	93.3%	N/A
Vendor X Leading email security vendor with URL protection enabled	55.2%	70.0%	49.3%
Proofpoint Proofpoint Essentials Business with URL Defense	33.3%	63.3%	21.3%
Microsoft Microsoft 365 Defender (formerly known as Microsoft ATP) with Safe Links	32.3%	56.7%	22.7%

Note: 105 total samples, 30 from PhishTank and 75 from the SlashNext AI Phishing Detection Database. Microsoft delayed delivery not enabled. Vendor X was an informal test to provide an additional data point for informal reference.

Source: Tolly, December 2020

Figure 1



Test Results

For an anti-phishing solution to be effective, it must have strong efficacy against spear phishing attacks. Spear phishing emails are sent in low volume to specific target addresses and are sent from sources where the sending domain and IP address do not have negative reputations. These characteristics make it difficult for anti-phishing solutions to detect because it bypasses the security layer that relies on email volume and reputation.

The test was very focused and straightforward. The test and its results can be described quite succinctly. Just over 100 threat URLs were selected for testing from the PhishTank community site and the SlashNext AI Phishing Detection Database. All specific URLs were chosen by Tolly. For details of test configuration and process see Test Setup & Methodology section.

Overall, SlashNext had an accuracy of 98.1% which was more than 3x of Proofpoint and Microsoft and nearly 2x that of Vendor X.

SlashNext correctly identified 93.3% of the PhishTank URLs compared with between 56% and 70% for the other email security solutions.

SlashNext claims they identify zero-hour phishing URLs much earlier than other vendors and has a more comprehensive offering. To evaluate this, 75 recent URLs were chosen from their AI Phishing Detection Database and used to test the other vendors.

Proofpoint and Microsoft accurately identified from 21% to 23% of these and Vendor X accurately identified only 49% of these.

According to SlashNext, the company is solely focused on phishing protection, including hard to detect spear phishing attacks missed by others. SlashNext's patented technology utilizes virtual browsers, computer vision and natural language processing (NLP) machine learning (ML).

Phishing is the Number One Threat Action in Breaches

The number one cause of a cybersecurity breach is phishing, and this year the average cost of a corporate breach was \$2.8 million, making phishing an urgent issue. Yet, many organizations do not see phishing as their biggest concern and do not use the latest technology to defend against today's sophisticated phishing attacks.

According to Gartner¹, a dramatic increase in phishing attacks' volume and success require a reevaluation of security controls, and recommends solutions that use computer vision to protect against account take over attacks. Additionally, the significant shift to remote working continues to fuel the adoption of cloud services and other collaboration tools beyond email. These are likely to become additional attack vectors.

New Detection Technology is Required

Protecting remote workers from today's sophisticated attacks requires a phishing protection toolbox that takes a zero-trust approach covering several attack vectors and goes beyond URL inspection and domain reputation.

Cybercriminals use automation and AI to increase the likelihood of compromising a target by leveraging legitimate infrastructure and matching data to build detailed lists of targets to increase their success. The Gartner Email Market Report cites security supplements that use computer vision machine learning to ensure protection against the changing threat landscape.

Comprehensive Communication Channel and Phishing Payload Protection

Phishing attacks are growing because they are no longer just an email problem and has expanded to SMS/iMessage, social networks, collaboration platforms, videoconferencing, and gaming services. Cybercriminals have expanded their attack payloads beyond credential theft to scareware, social engineering scams, rogue software downloads and fraudulent ads. Mobile users are particularly vulnerable because of small screens, users' mistakes, and invisible URL strings hiding the address. According to the 2020 Verizon Data Breach report, iPhone users are 18x more likely to get phished than to download malware.

1: Gartner Market Guide for Email Security, Published 8 September 2020 - ID G00722358

Source: SlashNext, January 2021



Test Setup & Methodology

Testing was conducted in late December 2020. Security gateway systems were implemented via cloud services using then-current systems.

System Configuration

SlashNext

SlashNext (v2.1.291) ran as a plugin on Google Chrome browser (v87.0.x). SlashNext was configured to interact with all sites visited.

Microsoft Defender (Safe Links)

Defender, formerly known as Microsoft Advanced Threat Protection or ATP, was tested using a Microsoft 365 email environment with E5 licensing. The following relevant "Safe Links" options were used: 1) URL rewriting was enabled, 2) Real-time URL scanning was enabled but "Wait for URL scanning to complete before delivering messages" was not enabled, and 3) "Do not allow users to click through to original URL" was enabled.

Proofpoint Essentials Business (URL Defense)

All testing was done using Proofpoint Essentials Business with its URL Defense feature.

The default URL Defense settings were used. These settings include: 1) "Rewrite URLs that are located in DKIM signed messages" as enabled, and 2) "Exclude re-writing bare IP addresses in plain text emails" as enabled.

Vendor X

This system was configured with URL protection enabled as was evident in the emails delivered during the test. Tolly did not configure or have access to the actual configuration of this system. Thus, this test is to be considered an informal test to provide another informational data point.

Test Corpus

105 samples were tested in total. 30 samples were selected from the PhishTank community site and 75 were selected from the SlashNext AI Phishing Detection Database. All specific samples were chosen by Tolly. All URLs tested, modified to be safe, are listed on the following pages.

PhishTank URLs. Prior to each test, Tolly reviewed the most recent submissions to PhishTank and chose one for the given test. Of the PhishTank URLs, several were deemed by Tolly to be benign when tested. For those false positives the correct action was to allow click through to the URL.

SlashNext categorize phishing into five payload types: credential theft, social engineering scams, scareware, rogue software apps & extensions and communication callbacks. Tolly selected 15 recent URLs from each category for the test. The URLs used are listed on the following pages with modifications made so that the reader can avoid inadvertently triggering a malicious URL. It is important to note that phishing URLs and results will change over time. Thus, a person running a test on the same URLs used by Tolly at a later date may well get different results.



Test Process

Each test message was sent from a single source email address to target addresses in each of the systems being evaluated. Thus, all systems received the URLs at the same time. Each email system was accessed immediately after the message was sent so that the tester could evaluate the URL protection responses to the time-of-click action.

The same source email address was used for all tests. Several minutes elapsed between each test. During this time three benign emails were sent to the same set of recipients. Test engineers confirmed that these benign messages were all received.

Phishing accuracy was determined as follows: If an email containing a phishing URL did not arrive in the destination inbox or spam folder for any reason, because it was quarantined or deleted, it was deemed an accurate detection. If an email with a threat arrived but was blocked on click, it was deemed an accurate detection. If click through was allowed on a malicious, rewritten URL, that test was deemed a failure.



URLs Tested - Part 1

PhishTank

hxxps://billings-myeel[.]com/account/index?ac=ee

hxxps://storage[.]googleapis[.]com/well-argo/index[.]html

hxxps://sexsamasya[.]co[.]in/CD/office365[.]htm

hxxp://peytel24[.]net/494612

hxxps://myee-mobileverify[.]com/

hxxp://withyoumall[.]websitesamazon[.]site/

hxxps://myeebilling-updates[.]com/

hxxp://hayagrivaacademy[.]com/css/index[.]php

hxxps://confirm-90002034245219[.]tk/checkpoint_next[.]html?Facebook_Update=

hxxp://amazon[.]top[.]kfxwpw[.]cn/

hxxps://online[.]pessoafiscacaixaeconomica[.]site/web/acao[.]php

hxxp://notification-recovery-officer-identity-supports[.]my[.]id/pages[.]php

hxxps://docs[.]google[.]com/forms/d/e/1FAIpQLSc7aqPu7jNlneRTenHHCaBeITAZl6LWHwUuLS-BPZ9kGJtkcA/viewform?usp=sf_link

hxxps://my[.]jcb[.]co[.]scdpq[.]com/index[.]html

hxxp://www[.]jeposccrd[.]cc/

hxxps://materialdelay[.]com/[.]access[.]american[.]exp/amex/secure/?id=0895fba75455a032a958b2ae2ad3faaa0895fba75455a032a958b2ae2ad3faaa0895fba75455a032a958b2ae2ad3faaa

hxxps://kjasdghf[.]xyz/

hxxp://243230[.]dlaiemkamzds[.]com/

hxxps://fghghfjytrel[.]buzz/

hxxp://notification-identity-officer-recovery-support[.]my[.]id/pages[.]php

hxxp://olx-pl-id[.]ru/

hxxps://www[.]db-webank[.]com/

hxxps://docs[.]google[.]com/forms/d/e/1FAIpQLSfQGeCRanHlI7YpSaw12a9kH7LjnaRHck0tCurqV_iWZUEfBA/viewform?vc=0&c=0&w=1&flr=0&usp=mail_form_link

hxxps://activobank-pt[.]site/

hxxp://47[.]88[.]76[.]58[.]caixa

hxxps://amazon-nz[.]online/

hxxps://fineststitch[.]com/citi/citibank/

hxxps://pl[.]olx-cash[.]online/cash32193051

hxxp://www[.]activacionesbancolombias[.]com/

hxxp://bancovotorantim[.]aprovar[.]site/

SlashNext (1 of 3)

hxxp://www431[.]ifthecomm[.]xn--i1ammyc[.]xn--p1ai/

hxxp://www579[.]wrgoree[.]xn--i1akppahyl[.]xn--p1ai/

hxxps://soulsparke[.]global/wp-content/uploads/mainfile/section[.]php?stone=k9ah9qnug990wf&family=cut&ten=reach

hxxp://goole3i[.]com/fbsb

hxxp://musk-crypto[.]fund/

hxxp://live[.]1-loto[.]site/

hxxp://prize[.]1-vk[.]site/

hxxp://eng[.]1-gift[.]site/

hxxps://num[.]wsyamp[.]buzz/ssn_h847/index_ru[.]php

hxxp://www[.]bulbgossip[.]cyou/Kkwocwk/pvgkf776896jescata/-H67VN6vCWpdDg9ip_Jv0w3x52IXiGvvLVN3Wt3wqY/p0exbKw4qUj6MNjYvz0DCu3USle1TiUoCksmDfMApoaWrvDhlu0VKPqAMwCO4NbVfHJ3CYx_0Skdqi_Nf05t2xaDp3pGc_7C0XEmGuTc2jzMXkBXaPbeTEhKvaUc2

hxxps://claimdiamond[.]e22[.]25u[.]com/

hxxps://nam11[.]safelinks[.]protection[.]outlook[.]com/?url=hxxp%3A%2F%2Fpaypal[.]xn--80abcv6bn6e[.]xn--p1ai%2F&data=04%7C01%7Ckevin%4033yrs[.]onmicrosoft[.]com%7C19f52a421feb4d66965308d8ac3c81e%7C63e40c3f08c24b79a2eb4b371933daeb%7C0%7C0%7C637449510328869904%7CUnknown%7CTWFpbGZsb3d8eyJWoiMCAwLjAwMDAilCjQjoiV2luMzliLjBtIl6lK1haWwiLCjVCl6Mn0%3D%7C1000&sdata=OKEgXgHeopxG%2BybZMdqoqxley0AJ4Ydivh%2Fq%2BVra8%3D&reserved=0

hxxp://luck-lucky[.]buzz/cc

hxxps://www[.]www[.]www[.]us-east-4www[.]blockchain[.]com--autotargeting[.]biolinok[.]com/

hxxps://relampagopromo[.]online/PRODUTO462724true/produto[.]php?linkcompleto=hxxps://www[.]americanas[.]com[.]br/produto/1746133387?pfm_carac=Galaxy%20M31&id=1

hxxp://imp[.]searchcll[.]com/impression[.]do?source=1&sub_id=20171212&useragent=mozilla/5[.]0+(windows+nt+6[.]1;+wow64;+trident/7[.]0;+rv:11[.]0)+like+gecko&traffic_source=appfocus35&user_id=f6e26a88-8a29-41cb-8351-9f6a611d4426&implementation_id=classifieds__1[.]30&subid=11[.]0[.]9600[.]19572&event=ex_executed

hxxp://imp[.]searchdirma[.]com/impression[.]do?source=display&sub_id=20170203&useragent=Mozilla/5[.]0+(Windows;+U;+Windows+NT+5[.]1;+en-GB;+rv:1[.]8[.]1[.]6)+Gecko/20070725+Firefox/2[.]0[.]0[.]6&traffic_source=appfocus45&user_id=e2ef6b37-8de2-49afb-07-7e8a09e160f8&implementation_id=maps__1[.]GET

hxxp://imp[.]searchhighdrp[.]com/impression[.]do?source=32-bb8&sub_id=20170305&useragent=Mozilla/4[.]0+(compatible;+MSIE+8[.]0;+Windows+NT+5[.]1;+Trident/4[.]0;+[.]NET+CLR+2[.]0[.]50727)&traffic_source=appfocus157&user_id=a395f864-0476-47ec-8b17-b2de94a787fe&implementation_id=radio__1[.]30&event=ex_installed

hxxp://imp[.]yourfastemailnowpop[.]com/impression[.]do?source=b47e0b3c-d27e-4b33-a4ea-aeb9897bdfd1_1566041_v1-bb9&sub_id=20180422&useragent=Mozilla/4[.]0+(compatible;+MSIE+6[.]0;+Windows+NT+5[.]1;+SV1;+[.]NET+CLR+2[.]0[.]50727)&traffic_source=appfocus65&user_id=f76de375-105a-4c56-adcf-a7e34ea078b6&implementation_id=email__1[.]30&subid=11[.]0[.]9600[.]19572&event=ex_executed

Source: Tolly, December 2020



URLs Tested - Part 2

SlashNext (2 of 3)

hxxp://imp[.]searchjsmfd[.]com/impression[.]do?source=%7Bparam%7D-bb9&sub_id=20180422&useragent=Mozilla/4[.]0(compatible&traffic_source=appfocus84&user_id=b2c108f6-c8e5-4845-9222-2ea24e7ecb8&implementation_id=maps_1[.]30&subid2=6[.]0[.]2900[.]J5512&event=ex_set_hp

hxxp://imp[.]myradioxp[.]com/impression[.]do?source=766408&sub_id=20170206&useragent=Mozilla/5[.]0+(Windows;+U;+MSIE+9[.]0;+Windows+NT+9[.]0;+en-US)+AppEngine-Google;+(+hxxp://code[.]google[.]com/appengine;+appid:+s~virustotalcloud)&traffic_source=AppFocus31&user_id=1ae14de9-3279-4411-a174-9c068fe944b3&implementation_id=radio_1[.]30&event=ex_installed

hxxp://imp[.]yourtransitinfonowpop[.]com/impression[.]do?source=1fc39a2c-8085-43ba-af90-e91a52b5544c_680702_v1-bb9&sub_id=20180422&useragent=Mozilla/4[.]0+(compatible&traffic_source=appfocus65&user_id=cdaa9591-f323-4ed5-8df6-b32a88c628d6&implementation_id=transit_1[.]30&subid2=11[.]0[.]9600[.]J19572&event=ex_executed

hxxp://imp[.]hthelocalclassifieds[.]co/impression[.]do?source=s-ccc2-lp0-bb8&sub_id=20180417&useragent=mozilla/5[.]0+(windows+nt+10[.]0;+wow64;+trident/7[.]0;+rv:11[.]0)+like+gecko&traffic_source=appfocus1&user_id=a621abc0-6218-4ec9-8cf3-2935186053c7&implementation_id=classifieds_spt_1[.]30&offer_id=ts1&subid2=11[.]0[.]9600[.]J19572&event=ex_executed

hxxp://imp[.]htv-now[.]co/impression[.]do?source=g-ccc2-lp0-bb9&sub_id=20180417&useragent=mozilla/5[.]0+(windows+nt+10[.]0;+wow64;+trident/7[.]0;+rv:11[.]0)+like+gecko&traffic_source=appfocus1&user_id=12a910a3-6f45-4490-bc42-3a7944f32929&implementation_id=tv_spt_1[.]30&offer_id=ts1&subid2=11[.]0[.]9600[.]J19572&event=ex_executed

hxxp://imp[.]searchrmgni2[.]com/impression[.]do?source=_v1-bb8&sub_id=20180418&useragent=Mozilla/4[.]0+(compatible;+MSIE+6[.]0;+Windows+NT+5[.]1;+SV1;+NET+CLR+2[.]0[.]J50727)&traffic_source=appfocus35&user_id=37980db-f3a8-4b13-9057-41e0d64d38a8&implementation_id=news_1[.]30&subid2=6[.]0[.]2900[.]J55GET

hxxp://imp[.]hdopplerweatherradar[.]co/impression[.]do?source=g-ccc3-lp0-bb9&sub_id=20180417&useragent=mozilla/5[.]0+(windows+nt+6[.]1;+wow64;+trident/7[.]0;+maau;+rv:11[.]0)+like+gecko&traffic_source=appfocus1&user_id=a8cfbcf-2bfc-466d-becf-5a4acb333bb8&implementation_id=weather_spt_1[.]30&ofGET

hxxp://imp[.]couponsimplified[.]com/impression[.]do?source=(network)-SL1-googlepartners&sub_id=20171021&useragent=Python-urllib/2[.]6&traffic_source=appfocus1&user_id=7094289b-d38a-4121-a416-6409351a433d&implementation_id=coupons_1[.]30&event=ex_installed

hxxp://imp[.]yourrecipenow[.]com/impression[.]do?source=Yahoo&sub_id=20170131&useragent=Mozilla/5[.]0+(Windows;+U;+MSIE+9[.]0;+Windows+NT+9[.]0;+en-US)+AppEngine-Google;+(+hxxp://code[.]google[.]com/appengine;+appid:+s~virustotalcloud)&traffic_source=AppFocus154&user_id=16772d05-6d22-4752-be15-1b1fd71c9413&implementation_id=recipes_1[.]30&event=ex_installed

hxxp://imp[.]searchfreedm[.]com/impression[.]do?source=250&sub_id=20170321&useragent=Mozilla/4[.]0+(compatible;+MSIE+8[.]0;+Windows+NT+5[.]1;+Trident/4[.]0;+NET+CLR+2[.]0[.]J50727)&traffic_source=appfocus157&user_id=d1959090-250c-491c-9090-3b38df6dda2&implementation_id=maps_1[.]30&event=ex_inGET

hxxp://imp[.]getfitnow[.]co/impression[.]do?source=&sub_id=20170209&useragent=Mozilla/5[.]0+(Windows+NT+6[.]1;+Trident/7[.]0;+rv:11[.]0)+like+Gecko&traffic_source=appfocus1&user_id=8002b0d8-bc14-43c0-9af7-44c1095efda4&implementation_id=fitness_1[.]30&event=ex_installed

hxxp://luckyspinnewow[.]ga/

hxxps://www[.]secure-lkb[.]xyz/

hxxps://claimseventsmoonon-30[.]cf/

hxxp://pubgwin[.]tk/verification[.]php

hxxps://www[.]helpcontactsupport[.]com/accounts/login/

hxxp://satomiki[.]org/tax/home[.]php

hxxps://2802b8f3adbb[.]ngrok[.]io/

hxxps://Instagramhelpcenterservices[.]ml/

hxxp://womensfashionnow[.]com/login[.]html

hxxps://evafoams[.]in/wp-admin/wp-admin/Recovery8[.]1[.]3/source/index[.]php?email=Jackdavis@eureliosolutions[.]com

hxxp://tammyjohnsphotography[.]com/cnpp/login[.]jsp[.]php

hxxp://bethraymond32[.]com/mazon/amazon

hxxp://whatsapp-grupp-viral[.]tk/

hxxp://www[.]u972975c2r[.]ha005[.]t[.]justns[.]ru/TjY8SK47u5h6EdV9n9bLvaB68c/c577cb1b38f4765/region[.]php?AUTH=c577cb1b38f4765

hxxps://87[.]gadget-errors2[.]com/0203-av/?to=0203-av&campid=71366bbc-ebf4-4c68-9af1-c2cd26859637&utm_source=ZPK&landerid=b082b3e9-6657-4b76-976e-63a3aad1065c&bv=Android%20Webview&lander=1305-intermediary-lander%20-%20[MSF]&pccid=d6ur7dv30jf8h4f4ilh5o3dc&phone_brand=Huawei&model=Mate%2020%20X&zone_id=foxtrot-him-MymHcFHB&supply_id=&camp_id=best%20deal&source=argent-porcupine&ua=lander&creative=0&ismf=1&pathid=088abeb8-8e62-7498-f5e9-54102f785594&brand=av

hxxp://xq3o[.]streaming[.]content4you[.]net/

hxxp://answer2unlock2020[.]com/1694?id=5bb9bbb3-808f-4ed6-a228-175fd363755a&h=17183#warning

Source: Tolly, December 2020



URLs Tested - Part 3

SlashNext (3 of 3)

- hxxps://wmcpt[.]oductevidel[.]space/IWOURI?tag_id=864384&sub_id1=1235&sub_id2=3834460451238802127&cookie_id=0365fa37-4afa-4a57-bac4-f1be408338a0&lp=oct_11&tb=redirect&allb=redirect&ob=redirect&href=hxxps%3A%2F%2Ficcompanzens[.]fun%2F%3Ftid%3D864897%26noocp%3D1%26subid%3D1235&ge o=KR
- hxxps://93[.]gadget-errors2[.]com/0203-av-cmpl-wh/
- h x x p s : / / u n d o u p g r a d e 2 4 [.] y o u r g r e a t f r e e d o w n l o a d s o u r c e [.] i n f o / a l k ? k i u y = y - K m T z P d Y P C n P e O Z I A r L b _ 2 C T v h Y M c d X 5 M w j b T l p G 3 Q [.] & c i d = 8 8 1 8 6 6 6 1 1 6 1 3 9 5 3 1 3 6 7 & s u b = 6 7 5 4 5 9 & a p p _ i d = 1 0 0
- hxxps://installupgrade[.]yourgreatfreedownloadsource[.]info/nalp?plan=wsBY6ra7uCNtbQThKSDOTuZolnELE2flB5BPz7WKEiA[.]&cid=%7Bs2sparam%7D&sid=%7Bsiteid%7D
- hxxps://pulsagrat[.]website/link/gjisel/
- hxxps://feelgoodup[.]com/apps/ss_lp1/index[.]html
- hxxp://tliveradiopro[.]com/
- hxxps://tv5[.]live/
- hxxp://searchmmd5[.]com/
- hxxp://fastmapdirections[.]com/
- hxxps://bestvpnprotection[.]com/landers/av_lockvpn_lp1_black_red_5_en_new/index[.]html
- hxxp://among-us-hack[.]ml/
- h x x p : / / g o o g l e [.] c o - 1 [.] o n l i n e / a n d r o i d / g o o d [.] p h p ? & m o d e l = & i p = 1 0 4 [.] 2 2 7 [.] 1 2 9 [.] 1 5 7 & c a m p i d = 2 8 4 8 6 5 8 5 - d 9 3 5 - 4 0 1 a - a 2 b 6 - 0 5 b d 7 3 a 3 d 3 c d & b r o w s e r = C h r o m e & & b r o w s e r v e r s i o n = C h r o m e % 2 0 6 7 & c i t y = B u f f a l o & o s = W i n d o w s & t d = 8 w f 8 p [.] b e m o b t r c k s [.] c o m & u a = M o z i l l a % 2 F 5 [.] 0 % 2 0 (W i n d o w s % 2 0 N T % 2 0 1 0 [.] 0 % 3 B % 2 0 W O W 6 4) % 2 0 A p p l e W e b K i t % 2 F 5 3 7 [.] 3 6 % 2 0 (K H T M L % 2 C % 2 0 L i k e % 2 0 G e c k o) % 2 0 C h r o m e % 2 F 6 7 [.] 0 [.] 3 3 9 6 [.] 7 9 % 2 0 S a f a r i % 2 F 5 3 7 [.] 1 6 & l a n g u a g e = e n & c o n n e c t i o n = C o r p o r a t e & i s p = S e r v e r M a n i a & c o u n t r y = U n i t e d % 2 0 S t a t e s & c e p = & b e m o b d a t a = c % 3 D 2 8 4 8 6 5 8 5 - d 9 3 5 - 4 0 1 a - a 2 b 6 - 0 5 b d 7 3 a 3 d 3 c d [.] [.] a % 3 D 0 [.] [.] b % 3 D 0
- hxxp://51[.]91[.]147[.]243/1201246879871200136698520125741542/data/erreur/fr-fr/windows/15254879882001332975
- hxxp://51[.]91[.]150[.]243/1201246879871200136698520125741542/data/erreur/fr-fr/windows/15254879882001332975
- hxxps://ebmxf[.]thesciencebank[.]com/4502/ff/
- hxxp://get[.]wizbyte[.]xyz/
- hxxps://distribution-labs[.]com/it?cost=[PRICE]&cy=usd&external_id=[CLICK_ID]&creative_id=[BANNER_CREATIVE_ID]&ad_campaign_id=[CAMPAIGN_ID]&source=[DOMAIN]
- hxxps://www[.]ebriefday[.]online/5541def_Edge_New_updated/Winhelpxcode8080xwinEDerrorxxdc/
- hxxps://qmfff[.]hotelluxuria[.]com/4502/ff/
- hxxp://websys1548[.]xyz/arsel/WIn01sec0R999ity0CHSys01888Y
- hxxp://139[.]59[.]124[.]188/
- hxxp://hygfewj764[.]cf/
- hxxp://www[.]computer-hulplijn[.]nl/
- hxxp://206[.]189[.]85[.]205/
- hxxp://japan-hd00041201[.]online/vcfsty[.]online/otchr01-g245644s6-x546s-sf5s98dv4x-vx5d46-xv5x5787s64-x5874sw-xs54a-ewref/POP/index[.]html
- hxxp://spaceshellvpn[.]com/landers/6734cd79fc/index[.]html

Source: Tolly, December 2020



About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:

<http://www.tolly.com>

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

tb-1-wt-2021-01-22-VerH