



Darryl M. Woo
415.733.6068
DWoo@goodwinlaw.com

Goodwin Procter LLP
Three Embarcadero Center
San Francisco, CA 94111
Goodwinlaw.com
T: 415.733.6000

August 6, 2020

VIA EMAIL AT GLOBALSUPPORT@ICANN.ORG

ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
Globalsupport@icann.org

Re: **GalComm False and Misleading Claims**

Dear Sir or Madam,

This firm represents Awake Security, Inc. (“Awake”). I am writing with reference to the submission of a copy of a letter to ICANN on behalf of Communigal Communication Ltd. d/b/a GalComm (“GalComm”). In that letter, copy attached for reference, counsel for GalComm makes baseless and misleading allegations that Awake has made false and disparaging statements regarding GalComm. In particular, GalComm’s letter takes issue with Awake’s report entitled, “The Internet’s New Arms Dealers: Malicious Domain Registrars” (the “Report”), as well as a June 25, 2020 YouTube presentation by Awake entitled “The New Rootkit: How Malicious Chrome Extensions Enabled a Global Surveillance Campaign” (the “Presentation”).

Upon receipt of GalComm’s letter, Awake responded to GalComm about the Report and Presentation, explaining how their allegations were utterly without basis. As it appears that GalComm has not provided you with a copy of Awake’s response, we attach a copy in the hopes that it will dispel any notion that Awake engaged in anything other than a legitimate investigation into multiple independent complaints regarding GalComm and many of its hosted web domains.

This letter is not intended to contain a complete statement of facts with respect to the subject matter hereof, and Awake does not waive any legal or equitable rights, remedies, claims or defenses available to it, all of which are expressly reserved.

Sincerely,

A handwritten signature in blue ink, appearing to be 'Darryl M. Woo', written over a horizontal line.

Darryl M. Woo
Todd Marabella
Encls.



Darryl M. Woo
415.733.6068
DWoo@goodwinlaw.com

Goodwin Procter LLP
Three Embarcadero Center
San Francisco, CA 94111
Goodwinlaw.com
T: 415.733.6000

July 27, 2020

VIA EMAIL AT DN@NEWMANLAW.COM

Derek A. Newman
Newman DuWors LLP
100 Wilshire Blvd, Suite 700
Santa Monica, CA 90401

Re: GalComm Claims of Defamation

Dear Mr. Newman,

This firm represents Awake Security, Inc. (“Awake”). I am writing with reference to your July 21, 2020 letter (the “Letter”) on behalf of Communigal Communication Ltd. d/b/a GalComm (“GalComm”) in which you allege that Awake has made false and disparaging statements regarding GalComm and its services in its report entitled “The Internet’s New Arms Dealers: Malicious Domain Registrars” (the “Report”) as well as in a June 25, 2020 YouTube presentation entitled “The New Rootkit: How Malicious Chrome Extensions Enabled a Global Surveillance Campaign,” (the “Presentation”).

Upon review of your letter and the referenced media, we most strongly disagree. As you are well aware, the truth is an absolute defense to claims of defamation. Here, because each of the statements you highlight in your letter are either not disparaging at all, or were true at the time they were made, GalComm has no actionable claim of defamation.

At the outset, let me provide some context about Awake and its processes. Awake has developed a strong reputation in the market for improving the security of the Internet. As part of its mission to improve Internet security, Awake publishes reports on vulnerabilities found in various platforms and service providers. As but one example, Awake notified Google of security issues that Awake discovered in generating a report on the platform, and Awake’s report led to Google choosing to engage with Awake to resolve the reported issues. This outcome – the improvement in security of the Internet as a whole – has always been Awake’s goal in publishing its reports.

I. Awake Contacted GalComm Prior to the Publication of the Report

In your Letter, you allege that Awake’s claim that it attempted to contact GalComm prior to publication of its Report to be “false and harmful to GalComm.” This is demonstrably untrue. According to the attached forensic and audit logs procured through Awake’s Microsoft Exchange Services eDiscovery Platform, GalComm clearly received at least six copies of notifications from Awake about the abuses

Derek A. Newman
Newman DuWors LLP
July 27, 2020
Page 2

catalogued in the Report and Presentation. Moreover, not only did Awake make multiple attempts from April 29 to May 8, 2020 to contact GalComm, but we have evidence from Microsoft that shows that each of these notifications was successfully received by GalComm.

These were not the only efforts by Awake to reach out to GalComm ahead of publication regarding Awake's investigation. In fact, Awake consistently tried to provide GalComm the opportunity to review, comment on, and address the data disclosed in the Report. GalComm simply did not respond. Over the period of six weeks, Awake submitted myriad notices to the email address provided on GalComm's website; to the complaint submission form provided on that same website; and to GalComm's CEO (both via telephone and email) directly. As but one example, the third-party journalist working with Awake in generating the Report confirms that he delivered an email to GalComm's CEO with the full list of malicious GalComm domain names on June 15, 2020. Neither he, nor Awake, ever received a response.

II. The List of Domains Contained in the Report Was Truthful And Accurate When Made

In the Letter, you deny responsibility for any alleged malicious activity, in part because of your contention that 25% of the suspicious domains listed in Appendix A of the Report are not registered with GalComm and "have either been transferred out, deleted, or registered with a different registrar." Frankly, this response is non-sensical.

As noted in the Report itself, Awake's investigation extended from June 2019 to May 2020. Thus, while it may be true that *after* the Report was drafted and released, some domains may have been "transferred out, deleted, or registered with a different registrar," during the relevant time period, each and every one of the domains listed in Appendix A had GalComm as the registrar of record. This can be – and was – confirmed via third-party databases including, but not limited to VirusTotal, RiskIQ, WhoisXmlApi, which not only documented malicious activity for each listed website but also corroborated that GalComm was registrar during the period of the investigation.

Nowhere in the Report is there any representation that the list in Appendix A will remain unchanging forever. Indeed, given the rapid turnaround in malicious websites, the fact many of the domains listed in the Report may have been deleted or transferred (especially after the report was published) is not only unsurprising, it is irrelevant to the assessment of whether the statements in the Report were truthful.

III. A Registrar Is Responsible for the Abuse Perpetuated by Its Registrants

Your Letter goes on to argue that "[d]omain-name registrars, including GalComm, are neither expected nor required to evaluate the conduct of all of their registrant customers or the uses to which they put registered names" because there is "no requirement to do so in the standard Registrar Accreditation Agreement with ICANN." This is patently untrue.

Derek A. Newman
Newman DuWors LLP
July 27, 2020
Page 3

Section 3.18 (Registrar's Abuse Contact and Duty to Investigate Reports of Abuse) of the present ICANN Registrar Accreditation Agreement states that a registrar such as GalComm absolutely bears responsibility for “abuse involving Registered Names sponsored by Registrar.” It specifically requires not only that any registrar “take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse” but also that any reports regarding a malicious registrant “must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report.”

The Report does not suggest that GalComm has any responsibility beyond that established under ICANN. However, the fact that GalComm was the registrar of record for over 15,000 websites associated with malicious activities strongly suggests that GalComm has not been fulfilling its responsibilities. This is made especially clear given the Report’s truthful allegations that GalComm consistently ignored reports – from Awake and others – regarding the malicious and abusive acts of GalComm’s registrants. These actions alone support the truth of the claim that GalComm has abrogated its responsibilities under the ICANN Registrar Accreditation Agreement.

IV. The Purported “Smearing” of GalComm’s Reputation In the Report Is Based Entirely on the Accurate Reporting of Publicly Available Information Already Published by Others

Your Letter also alleges that the Report contains “false, irrelevant, and out-of-context issues” designed to “smear GalComm’s reputation.” Yet, the examples you provide are all instances where Awake simply and truthfully reported publicly available information already published by others. As but one example, you point to Chapter Four of the Report to complain of Awake’s inclusion of negative third-party reviews of GalComm and to characterize such reviews as false and irrelevant. Yet nowhere in your letter do you explain how or why Awake’s reporting of these reviews is inaccurate or deceptive. There is no evidence that Awake altered or otherwise edited the reviews to make them more negative or otherwise manipulated them to mislead a reader. Moreover, given that many of these negative user reviews were based on users’ dissatisfaction with GalComm’s slow or absent response to complaints of abuse or other malicious action on the part of GalComm’s registrants, the inclusion of these user reviews was extremely relevant to the claims made in the Report and in no way intended to “smear” GalComm in any respect.

Similarly, the Letter asserts that Awake defamed GalComm by referencing a Notice of Breach of the Registrar Accreditation Agreement sent by ICANN because the Report fails to note that “the notice was based on a misunderstanding that was resolved shortly thereafter.” However, while the Notice of Breach is a publicly available document, your claimed story of its resolution is not. Given GalComm’s refusal to respond to Awake’s numerous requests for review and comment, it is disingenuous in the extreme for GalComm to claim that Awake engaged in defamation by referencing the true and verifiable fact that GalComm received an ICANN Notice of Breach. Moreover, the inclusion of this factual event is extremely relevant as the Notice of Breach itself catalogues complaints from ICANN regarding GalComm’s dilatory and often completely absent responses to claims of abuse by its registrants. Thus,

Derek A. Newman
Newman DuWors LLP
July 27, 2020
Page 4

far from suggesting that the inclusion of this report provides evidence that Awake was untruthful in its claims that GalComm has enabled the malfeasance of its clients, it in fact further supports such claims.

You further claim that Awake's investigation of GalComm's association with BigNet Internet Solutions, Mobik, and webhostingservices.info is somehow also defamatory. First, as a threshold issue, due to GalComm's refusal to respond to Awake's communications, Awake was required to perform a detailed investigation of GalComm and its associates specifically to avoid making any untrue claims. During this investigation, Awake uncovered evidence of multiple domains that appear to have been registered with malicious intent via these associated companies. This is the basis for their inclusion in Appendix D to the Report.

Moreover, we note that your letter fails to suggest why the inclusion of these websites or Awake's investigation into GalComm's associates should be categorized as a false or misleading statement, and fails to point to any statements in the Report regarding these activities that would act as evidence of disparagement. Thus, it appears that we agree that Awake's investigation of these three entities does not trigger any liability under any laws.

V. The Presentation Does Not Contain False or Misleading Claims

Your Letter also takes issue with statements made during the Presentation given by Awake co-founder Gary Golomb. The majority of claims in the Letter are directed to statements regarding Awake's frustrated efforts to contact GalComm, either by itself or through the help of third-party journalists. For the reasons described above, these statements are neither false nor misleading, and instead truthfully and accurately reflect the many independent efforts undertaken by Awake to contact GalComm over the course multiple months prior to publication of the Report.

Additionally, you point to a comment regarding Awake's observation that "in a single day, more registrations were made than almost the previous year combined." While your Letter purports to provide "context" for that spike in registrations, at no point do you state or explain how this statement is false, misleading, or otherwise actionable. Similarly, you highlight a second statement from the Presentation regarding the fact that since the publication of the Report, many domains registered with GalComm that redirected users to malicious or abusive websites have changed and now redirect users to "more benign ad networks." Again, your letter makes no allegations as to why this statement should be viewed as false or misleading and how such a factual claim could be actionable as defamatory.

Awake takes allegations of defamation or disparagement seriously. It is for that very reason that Awake engaged in detailed and meticulous fact finding in the creation of its Report and it is why, as can be seen in the attached forensic files, Awake endeavored to reach out to GalComm over the course of six weeks in the hopes that GalComm would properly respond to the allegations therein. Based on your Letter, and the facts as we know them, any objective factfinder would conclude that Awake did not engage in any defamation or false and misleading advertising in its discussion of GalComm or its services. To the

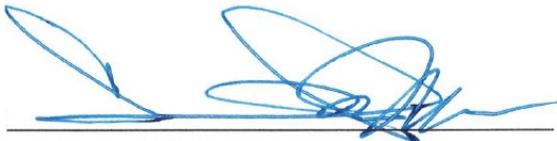
Derek A. Newman
Newman DuWors LLP
July 27, 2020
Page 5

extent that you disagree, we stand ready to review any evidence of actual false or disingenuous claims that you believe Awake has made and welcome the opportunity to discuss such evidence with you further. Given the difficulty in establishing the provenance of the type of evidence likely to be at issue here outside of formal discovery, however, we further request that any such evidence provided be forensically verifiable – as is the evidence provided along with this letter.

Unless and until such time as we receive any such evidence, we consider this matter closed. That said, in light of its mission to improve the security of the Internet, Awake is open to working with GalComm and its remediation efforts. For instance, Awake would be willing to consider publication of a further article or joint statement recounting GalComm’s remediation efforts based on Awake’s Report, i.e. to the effect that with the help of the examination conducted by Awake, GalComm was able to identify domain names associated with malicious activity and thus has been able to have them transferred out, deleted, or registered with a different registrar.

This letter is not intended to contain a complete statement of facts with respect to the subject matter hereof, and Awake does not waive any legal or equitable rights, remedies or defenses available to it, all of which are expressly reserved.

Sincerely,

A handwritten signature in blue ink, consisting of several loops and a long horizontal stroke at the end, positioned above a solid horizontal line.

Darryl M. Woo
Todd Marabella

ATTACHMENTS

Export Name galcomm emails_ReportsOnly
 Export ID ce4e3bad-4f86-458a-5817-08d82feba418
 Status The export completed successfully.
 De-Duplication Enabled No
 Export Location C:\Users\Moon\Downloads\Galcomm eDiscovery
 Exports\Reports\galcomm
 emails_ReportsOnly\07.24.2020-0951AM
 Remove RMS Protection NO
 Location with Results 1

Location that successfully downloaded 1
 Locations that failed to download 0

	Items	Size(GB)	Size(Bytes)
Estimated	5	0	140,129
Exchange Estimated	5	0	140,129
Downloaded	5	0	140,129

Item Downloaded Errors 0
 Item Downloaded Warnings 0
 Item Skipped 0

SharePoint folders not downloaded 0
 SharePoint pages not downloaded 0
 SharePoint list items downloaded as Csv
 files 0
 SharePoint download errors 0
 SharePoint downloaded items 0
 Download Started 7/24/2020 9:51
 Download Completed 7/24/2020 9:52

Locations	Location name	Custodians	Items	Size(GB)	Size(Bytes)
gary@awakesecurity.com	gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e	gary@awal	5	0	140,129

trace.log

[2020-07-24 16:52:23.0250][8][Information]: Export has started. Status
[2020-07-24 16:52:23.0719][1][Information]: UnifiedExportTool engine version:
15.20.1771.000, CLR version: 4.0.30319.42000.
[2020-07-24 16:52:23.0719][1][Information]: Current local time: 7/24/2020 9:52:23
AM, current UTC time: 7/24/2020 4:52:23 PM.
[2020-07-24 16:52:23.0739][1][Information]: OS version: Microsoft Windows NT
6.2.9200.0, processor count: 8, x64: True, working set: 128430080.
[2020-07-24 16:52:23.0739][1][Information]: Export name: galcomm
emails_ReportsOnly.
[2020-07-24 16:52:23.0788][1][Information]: ConstantProvider..Ctor: Registry not
found for constants
[2020-07-24 16:52:23.2613][7][Information]: Start progress controller loop.
[2020-07-24 16:52:23.3731][1][Information]: Effective downloader concurrency: 48
[2020-07-24 16:52:23.3770][6][Information]: Start result recorder loop.
[2020-07-24 16:52:25.1004][1][Information]: Source store id:
ce4e3bad-4f86-458a-5817-08d82feba418, job run id:
ce4e3bad-4f86-458a-5817-08d82feba418, scenario: GenerateReportsOnly, store version:
2015-09-25, create time 7/24/2020 4:07:19 PM.
[2020-07-24 16:52:25.3308][11][Information]: Requesting
data/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/Root.meta from Azure storage
[2020-07-24 16:52:25.4545][6][Information]: Completed server task statistics - id:
c0c4ef19-43b4-4271-9ff5-a9a157642c9e, workload: Exchange, custodian:
gary@awakesecurity.com, displayName: gary@awakesecurity.com, identifier:
gary@awakesecurity.com, contentFormat: Msg, archiveFormat: Zip,
mailboxLocationType: Primary, completeTime: 7/24/2020 4:10:44 PM, estimatedCount:
5, estimatedSize: 140129, transferredCount: 5, transferredSize: 140129,
failureCode: 0, failureSide: , failureType: , failureDetails: , executingServer:
BY5PR11MB3959.namprd11.prod.outlook.com.
[2020-07-24 16:52:25.7138][1][Information]: Server job tracker scan status:
AnyTaskHasScheduled: True; AnyTaskHasStarted: True; AnyTaskInProgress: False;
AnyTaskHasCompleted: True; AllTasksHaveCompleted: True; IsCancelled: False;
exportStarted: False.
[2020-07-24 16:52:25.7268][1][Information]: Found 1 server tasks.
[2020-07-24 16:52:25.7278][1][Information]: Kicking off server task
gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e.
[2020-07-24 16:52:25.7686][6][Information]: Start exporting
(gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e).
[2020-07-24 16:52:25.7686][6][Information]: Start enumerating items for
gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e.
[2020-07-24 16:52:25.8245][6][Information]: Finish enumerating items for
gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e, total items
enumerated: 1, time elapsed: 00:00:00.0556915.
[2020-07-24 16:52:25.8285][8][Information]: Downloading for
data/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDRBatch/BATCH0000/MSG0.batch.
[2020-07-24 16:52:25.8325][7][Information]: Start item exporter loop for
gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e.
[2020-07-24 16:52:26.0210][8][Information]: Processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG0

trace.log

.meta. (1_1/1 from gary@awakesecurity.com)
[2020-07-24 16:52:26.0280][8][Information]: Initializing Exchange reports only
writer for gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e
GenerateReportsOnly.
[2020-07-24 16:52:26.0439][8][Information]: Requesting
data/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/Folder.meta from
Azure storage
[2020-07-24 16:52:26.1207][10][Information]: Requesting
data/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR576742227280134145/Folder.meta from
Azure storage
[2020-07-24 16:52:26.2015][3][Information]: Requesting
data/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR72339069014638593/Folder.meta from
Azure storage
[2020-07-24 16:52:26.2912][13][Information]: Finish processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG0
.meta
[2020-07-24 16:52:26.2972][13][Information]: Processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG1
.meta. (1_2/1 from gary@awakesecurity.com)
[2020-07-24 16:52:26.2972][13][Information]: Finish processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG1
.meta
[2020-07-24 16:52:26.2972][13][Information]: Processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG2
.meta. (1_3/1 from gary@awakesecurity.com)
[2020-07-24 16:52:26.2992][13][Information]: Finish processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG2
.meta
[2020-07-24 16:52:26.3002][13][Information]: Processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG3
.meta. (1_4/1 from gary@awakesecurity.com)
[2020-07-24 16:52:26.3002][13][Information]: Finish processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR720857415355990017/BATCH0000/MSG3
.meta
[2020-07-24 16:52:26.3002][13][Information]: Processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR648799821318062081/BATCH0000/MSG0
.meta. (1_5/1 from gary@awakesecurity.com)
[2020-07-24 16:52:26.3002][13][Information]: Requesting
data/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR648799821318062081/Folder.meta from
Azure storage
[2020-07-24 16:52:26.3720][3][Information]: Finish processing item
metadata/c0c4ef19-43b4-4271-9ff5-a9a157642c9e/FLDR648799821318062081/BATCH0000/MSG0
.meta
[2020-07-24 16:52:26.3760][8][Information]: TracerScope.Enter: Initializing
serialization file: C:\Users\Moon\Downloads\Galcomm eDiscovery
Exports\Reports\galcomm emails_ReportsOnly\07.24.2020-0951AM\manifest.xml
[2020-07-24 16:52:26.3780][8][Information]: TracerScope.Exit (2 ms): Initializing
serialization file: C:\Users\Moon\Downloads\Galcomm eDiscovery

trace.log

Exports\Reports\galcomm emails_ReportsOnly\07.24.2020-0951AM\manifest.xml
[2020-07-24 16:52:26.3780][3][Information]: Finish item exporter loop for
gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e, time
elapsed: 00:00:00.3557688.
[2020-07-24 16:52:26.3790][3][Information]: Finish exporting
(gary@awakesecurity.com, Primary, c0c4ef19-43b4-4271-9ff5-a9a157642c9e), time
elapsed: 00:00:00.6103987.
[2020-07-24 16:52:26.3820][14][Information]: ActionBlock
ConcurrentServerTaskExporter RanToCompletion
[2020-07-24 16:52:26.3840][15][Information]: ActionBlock ItemDownloader
RanToCompletion
[2020-07-24 16:52:29.4130][6][Information]: Finish progress controller loop, time
elapsed: 00:00:00.0081643.
[2020-07-24 16:52:29.4140][8][Information]: Finish result recorder loop, time
elapsed: 00:00:00.0952804.
[2020-07-24 16:52:29.4160][1][Information]: TracerScope.Enter:
EdrmSerializer.SerializeRelationships
[2020-07-24 16:52:29.4210][1][Information]: TracerScope.Exit (4 ms):
EdrmSerializer.SerializeRelationships
[2020-07-24 16:52:29.4220][1][Information]: Finalizing Serialization File:
C:\Users\Moon\Downloads\Galcomm eDiscovery Exports\Reports\galcomm
emails_ReportsOnly\07.24.2020-0951AM\manifest.xml
[2020-07-24 16:52:29.4240][1][Information]: TracerScope.Enter:
EdrmSerializer.SerializeRelationships
[2020-07-24 16:52:29.4240][1][Information]: TracerScope.Exit (0 ms):
EdrmSerializer.SerializeRelationships
[2020-07-24 16:52:29.4240][1][Information]: TracerScope.Enter:
EdrmSerializer.SerializeRelationships
[2020-07-24 16:52:29.4240][1][Information]: TracerScope.Exit (0 ms):
EdrmSerializer.SerializeRelationships
[2020-07-24 16:52:29.4390][1][Information]: Perf Statistics: max cached content
size: 9915, current cached content size: 0, current cached content count: 0, total
memory to GC: 9270440, collection count: 4 1 0, private bytes: 110346240, working
set: 153427968, download queue length: 0, download connection count: 0
[2020-07-24 16:52:29.4449][1][Information]: Working folder cleaned up.
[2020-07-24 16:52:29.4549][7][Information]: Overall transfer speed: 1 item per
second.
[2020-07-24 16:52:29.4549][7][Information]: Export has completed. Status:
Processed.

SENT BY EMAIL AND FEDEX

July 21, 2020

Rahul Kashyap, CEO
Gary Golomb, CTO
Awake Security, Inc.
2901 Tasman Dr., Suite 205
Santa Clara, CA 95054
Email: rahul@awakesecurity.com
gary@awakesecurity.com

Re: Demand to Cease and Desist False and Disparaging Statements about GalComm

Messrs. Kashyap and Golomb:

We represent Communigal Communication Ltd., which does business as GalComm, the largest Israel-based ICANN-accredited domain-name registrar.

GalComm recently discovered that Awake Security has published a series of false and defamatory claims about GalComm's registrar business, including in at least the following:

- Awake's report titled "The Internet's New Arms Dealers: Malicious Domain Registrars" (Report), which expressly accuses GalComm of engaging in criminal activity by putting "malicious domains, malware, and exploitative content" on the internet.
- Awake's YouTube video, presented by Mr. Golomb, titled "The New Rootkit: How Malicious Chrome Extensions Enabled a Global Surveillance Campaign," posted on June 25, 2020 (Webinar).¹

The false information about GalComm in Awake's publications has caused serious, ongoing harm to GalComm's business. GalComm is committed to protecting its clients and partners, and values cooperation with security regulations to affirmatively prevent malicious activity. Yet Awake's misrepresentations have resulted in clients, business partners, and reporters, unnecessarily calling into question GalComm's reputation.

GalComm demands that Awake retract the Report and the Webinar, make a public statement that corrects misrepresentations and provides GalComm's responses to the accusations raised in the Report, and issue a public apology to GalComm for the harm caused by the inaccurate publications.

¹ <https://www.youtube.com/watch?v=a9yaSz1aj2Q>

The corrective statement and apology should be issued publicly with at least the same reach as the Report and the Webinar. And GalComm demands that Awake directly notify all registered participants of the Webinar and Report, ICANN, and media reporters with whom Awake had been in contact regarding the Report and Webinar, of the statement and apology.

A. Awake’s claim that it attempted to contact GalComm prior to publication of its Report is false and harmful to GalComm.

Awake claims that prior to its publication of the Report, it repeatedly attempted to contact GalComm about the domains at issue and associated malicious activity, and to obtain answers to certain questions: “after sending notifications via email, web form, and phone on April 29, 2020, then resending the notification again nine days later, we have received no response from GalComm at publishing time of this paper.”² This is false. GalComm has no records of any form of communication, at any point in time, from Awake.

GalComm was not afforded the opportunity to address or respond to any of the accusations in the Report prior to its publication, and was thus deprived of the ability to preserve and protect its reputation. Additionally, the implication that GalComm ignored accusations that it was engaged in malicious criminal activity risks further serious harm to its reputation and registrar business.

B. The Report falsely misrepresents GalComm’s responsibility for the alleged malicious activity.

Had Awake actually contacted GalComm prior to publication of its Report, it would have learned that many of the facts it intended to publish were false.

First, Appendix A of the Report lists 15,262 “GalComm registered” domains allegedly associated with malicious or suspicious activity. The list is inaccurate in that, as of June 18, 2020, 25% of the domains listed are not affiliated with GalComm in any way; these domains have either been transferred out, deleted, or registered with a different registrar. The remaining domains are not affiliated with GalComm beyond the fact that GalComm is solely the domain registrar—GalComm does not provide hosting or other services for these names. And GalComm’s role as the domain registrar does not implicate GalComm in any criminal or malicious activity attributable to the domains. Awake’s claims to the contrary are baseless.

Domain-name registrars, including GalComm, are neither expected nor required to evaluate the conduct of all of their registrant customers or the uses to which they put registered names. There is no requirement to do so in the standard Registrar Accreditation Agreement with ICANN. And registrars are similarly under no obligation to take any action—legal or otherwise—against their registrants except under particular circumstances involving a complaint about a particular registrant.

² Report at 25.

Second, the Report identifies several domains, including *cdnus.com* and *cdneu.com*, which it claims are linked to malware distribution.³ Those specific domains are registered to IronSource, a GalComm registrant customer. GalComm has no affiliation or connection to the IronSource domains. Its relationship to the domains is limited to its role as a registrar. The claims that the IronSource domains and subdomains are used to communicate with suspect or malicious domains, and that InstallCore is linked to malware, are inaccurate and do not implicate GalComm. However, GalComm took immediate action by contacting IronSource following its receipt of Awake's Report and, after performing manual and automated scans of the domains, IronSource has confirmed that the domains are secured. Similarly, GalComm has contacted all of the registrants of the 152 domains listed in Appendix C, 149 of which are registered to IronSource. As noted above, GalComm took immediate action and contacted IronSource, confirming that its 149 domains were secured. One of the remaining three domains had already been taken down at the time GalComm was made aware of the Report. Another domain was taken down and then re-activated after GalComm received confirmation from the registrant that the domain is secure. And GalComm took down the remaining domain after receiving no response from the domain holder.

Third, Chapter 3 of the Report focuses on "evasive techniques," including domain parking. The Report distinguishes between "malicious" parking pages and "benign" parking pages, and falsely suggests GalComm is responsible for the malicious parking pages. Whether a user is redirected to a malicious domain is in the control of the parking company hosting the domain web page, not the domain registrar. GalComm is simply the domain registrar for the parking pages. It does not host the domains and is not affiliated with any malicious activity attributable to the domains.

Fourth, Chapter 4 of the Report, titled "the GalComm Connection" is dedicated entirely to smearing GalComm's reputation with false, irrelevant, and out-of-context issues. For example, it states that, "unsurprisingly," reviews from GalComm registrants "trend towards significantly negative." The Report also points to a Notice of Breach of Registrar Accreditation Agreement sent by ICANN seven years ago. What the Report fails to note is that the notice was based on a misunderstanding that was resolved shortly thereafter. The Report also describes an unrelated complaint associated with a domain registrant whose actions are not attributable to GalComm, suggesting that "datapoints like this help paint a picture about the type of registrants (end users) seeking GalComm."⁴

Additionally, Awake questions the activities of three entities associated with GalComm, without any valid basis for doing so. GalComm's connection with these entities is publicly available information and there is nothing nefarious about them. GalComm acquired BigNet Internet Solutions several years ago, Mobik is a related entity, and *webhostingservices.info* is simply one of GalComm's landing pages. The domains listed in Appendix D do not relate to any security issue. Nevertheless, GalComm has forwarded the domains to their respective registrants, and has subsequently cancelled all domains listed in Appendix D.

³ *Id.* at 12.

⁴ *Id.* at 23.

C. GalComm’s responses to Awake’s questions posed in the Report.

Awake’s Report lists three questions it claims it attempted to ask GalComm prior to publication of the Report.⁵ While GalComm was never made aware of and has no records of any such attempts, it responds as follows:

1. “What is GalComm’s policy on taking down (or blocking) domains being used exclusively for malicious purposes?”

GalComm’s policies are available on its websites located at galcomm.com and galcomm.co.il. These policies include GalComm’s Registration Agreement⁶ and Abuse reporting tool⁷, which is designed to report complaints of abuse associated with a GalComm-registered domain name. The policies and abuse form are also linked in the footer of each webpage.

GalComm handles 100% of abuse complaints received, most of which tend to be unrelated to security issues. GalComm forwards all complaints to the respective domain owner, asking the domain owner to investigate the issue and provide a response within a reasonable time. If GalComm does not receive a response, it considers the extent of further action necessary. Where a complaint pertains to security and stability issues, the domain is likely to be taken down. If the registrant responds and describes affirmative actions that it has taken to address the complaint, then GalComm closes the complaint and takes no further action at that time. And if the domain is registered through a web-hosting company known to GalComm, GalComm notifies the appropriate entity of the complaint as well.

2. “How are the people behind these domains able to acquire so many of them through GalComm?”

As with other registrars, GalComm has a robust network of resellers and business partners that are granted API access to GalComm’s platform. Those resellers and business partners are able to register and manage domains through GalComm’s registrar platform consistent with ICANN’s policies.

3. “Given these domains account for approximately 60% of the total domains GalComm currently has on the internet, how could this go unnoticed by the company?”

The 60%—presumably referring to the 15,262 domains listed in Appendix A—is an inaccurate representation. Of the 15,262 listed domains, only 11,599 are registered at GalComm as of June 18, 2020. Approximately 25% of the domains listed in Appendix A have either never been registered at GalComm, have been transferred to another registrar, or have expired and subsequently re-registered with another registrar. The remaining domains listed represent about 10% of GalComm’s

⁵ *Id.* at 24.

⁶ <https://secure.galcomm.co.il/General/RegistrationAgreement.aspx>

⁷ <http://www.galcomm.com/abuse/>

total domains, contrary to the Report's suggestion that a majority of GalComm's domains relate to malware. Nevertheless, any activity attributable to domains registered with GalComm will go unnoticed unless a complaint about a particular domain is filed. As discussed above, a domain registrar is under no obligation to proactively monitor the activity of its domain registrants. Nor would it be possible for any registrar to do so given the sheer volume of domain name registrations and their wide variety of uses.

Finally, the Report discusses the "curious case of rtb-seller.com."⁸ This domain is not owned by GalComm nor does GalComm serve as the domain's hosting provider. GalComm is simply the sponsoring registrar. Thus, GalComm is not responsible for any action attributable to the domain. And IronSource has verified that this domain has been scanned and confirmed as secured.

D. Awake's Webinar about the Report also includes harmful misrepresentations about GalComm.

On June 25, 2020, Awake published the Webinar, discussing its investigation involving GalComm and explaining the accusations presented in the Report. As with the Report, the Webinar includes false statements that pose serious risk to GalComm's registrar business.

First, in the Webinar, Awake repeats its false claims that it attempted to contact GalComm by phone, web forms, and email on April 29, 2020 and May 8, 2020, prior to publishing the Report. As noted above, GalComm has no records of any such attempts, and was not made aware of the Report or the Webinar prior to their publication.

Second, Awake falsely claims in the Webinar that prior to publication of the Report, GalComm was contacted by a journalist working with Awake, given sufficient time to respond to the journalist's efforts, yet failed to do so. GalComm's first communication with the journalist occurred on June 14, 2020 via LinkedIn, which was followed by an email on June 15, 2020 from the reporter sent to the abuse@galcomm.com email address—the same address that Awake allegedly used in its failed attempts to contact GalComm. GalComm immediately responded to the reporter's email, welcoming any additional information that would allow GalComm to evaluate the domains at issue. The journalist responded with the list of domains on the evening of June 17, 2020, Israel Daylight Time. Awake published its report on the morning of June 18, 2020. Unaware of the Report's publication, GalComm responded to the journalist with its initial analysis of the domain list that same day.

Third, Awake points to a spike of domain-name registrations though GalComm, indicating that "in a single day, more registrations were made than almost the previous year combined." As discussed above, GalComm has a network of resellers and business partners that are provided with API access to GalComm's platform. These third parties are able to register and manage domains without access to GalComm's website. "Bulk" registrations are common in the domain industry. The registration spike referenced in the Webinar, in December 2019, was a result of a flash sale under a marketing

⁸ *Id.* at 25.

program in which GalComm participated. Such flash sales are customary in domain registrar marketing programs.

Finally, in the Webinar, Awake discusses changes to particular domains a week after the Report's publication, stating that domains "that previously redirected to exploitative pages are now *actually* parked or redirect to more benign ad networks." Other than GalComm's ordinary policies and management procedures, GalComm has not changed any of the domains following the Report's publication. GalComm has no control over the usage of the domains or their redirection by the domains' respective hosting servers.

E. Awake Security is liable for the ongoing harm its false and defamatory statements have caused GalComm.

Defamation occurs when a party creates (1) a publication that is (2) false, (3) defamatory, (4) unprivileged, and (5) causes damage.⁹ Awake's false statements about GalComm, including in the Report and Webinar, are defamatory. Awake published the Report and the Webinar. The publications contain false information about GalComm's alleged affiliation with criminal and malicious activity, inaccurately suggesting that GalComm is responsible for its registrants' activities. The Report has effectively damaged GalComm's reputation. GalComm has received numerous inquiries pertaining to the Report and the Webinar from its clients, business partners, and reporters. GalComm has had to provide detailed explanations to its clients and business partners as to why the information contained in the Report and the Webinar is false.

Awake may be similarly liable for intentional interference with prospective economic advantage. Under California law, a claim for intentional interference with prospective economic advantage exists where there is (1) an economic relationship between the plaintiff and a third party, with the probability of future economic benefit to the plaintiff; (2) the defendant's knowledge of the relationship; (3) an intentional act by the defendant, designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) economic harm to the plaintiff caused by the defendant's wrongful act.¹⁰ GalComm has a potential economic relationship with domain registrants and business partners, which Awake is aware of given the nature of the domain industry and the level of industry understanding demonstrated in its Report. The Report is designed to disrupt GalComm's prospective relationships, stating that Awake believes GalComm is "at best complicit in the threats described within this report." The Report and the Webinar have not only harmed GalComm's reputation, but have also disrupted and harmed GalComm's prospective relationships.

⁹ *Wong v. Jing*, 189 Cal. App. 4th 1354, 1369 (2010).

¹⁰ *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1153-54 (2003).

F. GalComm seeks an amicable resolution of this dispute through Awake Security's withdrawal of the Report and the Webinar and issuance of a public apology.

GalComm would prefer to amicably resolve this matter. To that end, we respectfully request that Awake Security retract the Report and the Webinar, and issue a public apology to GalComm.

Given the seriousness of Awake's accusations and the imminent harm they pose to GalComm's business and reputation, GalComm requires a response by no later than by Monday, July 27 at 5:00 p.m. Pacific. If we have not received a satisfactory response by then, GalComm will proceed as it believes necessary to protect itself.

We look forward to your prompt response.

Thank you.

NEWMAN DU WORS LLP

A handwritten signature in black ink, appearing to read 'Derek A. Newman', with a horizontal line above it.

Derek A. Newman