CYBER THREAT ANALYSIS

IRAN

Recorded Future®

By Insikt Group®

August 20, 2024

GreenCharlie Infrastructure Linked to US Political Campaign Targeting

Insikt Group has discovered a cluster of malicious network infrastructure used by Iran-backed GreenCharlie, which is reportedly linked to malware used in the recent targeting of US political campaigns.

GreenCharlie's victimology includes research and policy analysts, government officials, diplomats, and high-value strategic targets.

GreenCharlie highly likely operates at the behest of the Islamic Revolutionary Guard Corps' Intelligence Organization (IRGC-IO), and has overlaps with Mint Sandstorm, Charming Kitten, and TA453.

Analysis cut-off date: August 19, 2024

Executive Summary

In August 2024, open sources revealed that US political campaign officials and affiliates were targeted as part of Mint Sandstorm and APT42 operations. In this report, we discuss threat activity associated with the Iran-nexus group we track as GreenCharlie, which overlaps with Mint Sandstorm, Charming Kitten, and TA453. Recorded Future has tracked Iran-linked GreenCharlie activity and malicious infrastructure since 2020. Our global Network Intelligence capability has allowed us to identify and track a large and rapidly evolving cluster of infrastructure used to support GreenCharlie cyber-espionage campaigns. Now, we have been able to link this network to the recent targeting of US political campaigns.

GreenCharlie is associated (1, 2) with malware such as POWERSTAR (also known as CharmPower and GorjolEcho) and NokNok, which is used with targeted spearphishing operations. A report issued by Google-Mandiant (TAG) on August 14, 2024, included hashes for a malware sample it calls GORBLE, which uses GreenCharlie infrastructure for command-and-control (C2). Insikt Group analyzed GORBLE, POWERSTAR, and TAMECAT (a malware associated with APT42 by Google-Mandiant), and determined they are all variants of the same malware family. We note that Insikt Group tracks infrastructure that overlaps with APT42 as GreenBravo.

Throughout July and August 2024, Insikt Group used Recorded Future Network Intelligence to identify various Iran-based IP addresses that communicated with GreenCharlie infrastructure. This infrastructure was likely used for phishing activity, including potentially for testing and training. Additionally, it is highly likely that the threat actors used ProtonVPN and/or ProtonMail to enable their operations.

GreenCharlie used multiple dynamic DNS (DDNS) providers to register its infrastructure (as depicted in **Appendix A**). These providers include Dynu, DNSEXIT, and Vitalwerks. Furthermore, consistent with its known tradecraft, the group also abused the Namecheap provider to register various other domains that are part of the cluster Insikt Group has tracked since June 2024.

Key Findings

- From May 2024 onward, GreenCharlie registered a large number of dynamic DNS (DDNS) domains that have highly likely been used for targeted social engineering and phishing operations.
- Insikt Group has established a direct infrastructure link between GreenCharlie clusters and malware referred to in open sources as GORBLE, which is reportedly linked to the targeting of US political candidates.

- Analysis of Recorded Future Network Intelligence indicates that GreenCharlie threat actors likely used ProtonVPN or ProtonMail to enable their operations.
- Iranian IP addresses were identified communicating with GreenCharlie infrastructure, which is likely part of the operation's spearphishing component.
- GreenCharlie's victimology includes research and policy analysts, government officials, diplomats, and high-value strategic targets. While Insikt Group has not identified direct evidence of the targeting of US government and political campaign officials, open-source reporting has enabled us to establish a credible link.
- GreenCharlie highly likely operates at the behest of the Islamic Revolutionary Guard Corps (IRGC); due to its persistent and strategic remit, it is also likely to be associated with the Intelligence Organization of the IRGC (IRGC-IO).

Threat Analysis

Infrastructure Analysis

GreenCharlie infrastructure detections enable progressive tracking of threat activity believed to overlap with infrastructure used to deliver malware such as POWERSTAR, NokNok, and GorjolEcho, in addition to enabling social engineering and phishing attacks. Since May 2024, we observed the group register multiple dynamic DNS (DDNS) domains using a variety of providers that include Dynu, DNSEXIT, Vitalwerks, Cloud DNS, FreeDNS, and Dia Systems. GreenCharlie hosted most of the identified infrastructure in small clusters. However, in specific circumstances, domains uniquely resolved to IP addresses owned by different infrastructure providers. The majority of the infrastructure identified as part of this research was hosted on Scalaxy B.V. (AS58061) infrastructure. We also identified GreenCharlie infrastructure that used the OVHcloud (AS16276), Worldstream, NL (AS49981), M247 (AS9009), and Podaon SIA (AS211381) providers for hosting.

Insikt Group has continued to track GreenCharlie threat clusters since we last reported on the threat group in May 2024. We observed that GreenCharlie continues to register infrastructure via the Namecheap registrar (much of which is highly likely active) using themes that overlap with cloud platforms, file sharing services, document visualization services, video conferencing, and authentication-themed domains. These include domains that use terms like “cloud”, “uptimezone”, “doceditor”, ”joincloud”, and “pageviewer”, among others.

GreenCharlie uses a multitude of top-level domains (TLDs) for domain registration. In the past we have detected .xyz, .icu, .network, .online, and .site domain clusters registered by the group. As it pertains to the cluster in this report, the majority were registered using the .info TLD. According to Recorded Future datasets, as well as DomainTools, GreenCharlie threat actors used WHOIS privacy protection to obfuscate registration details.

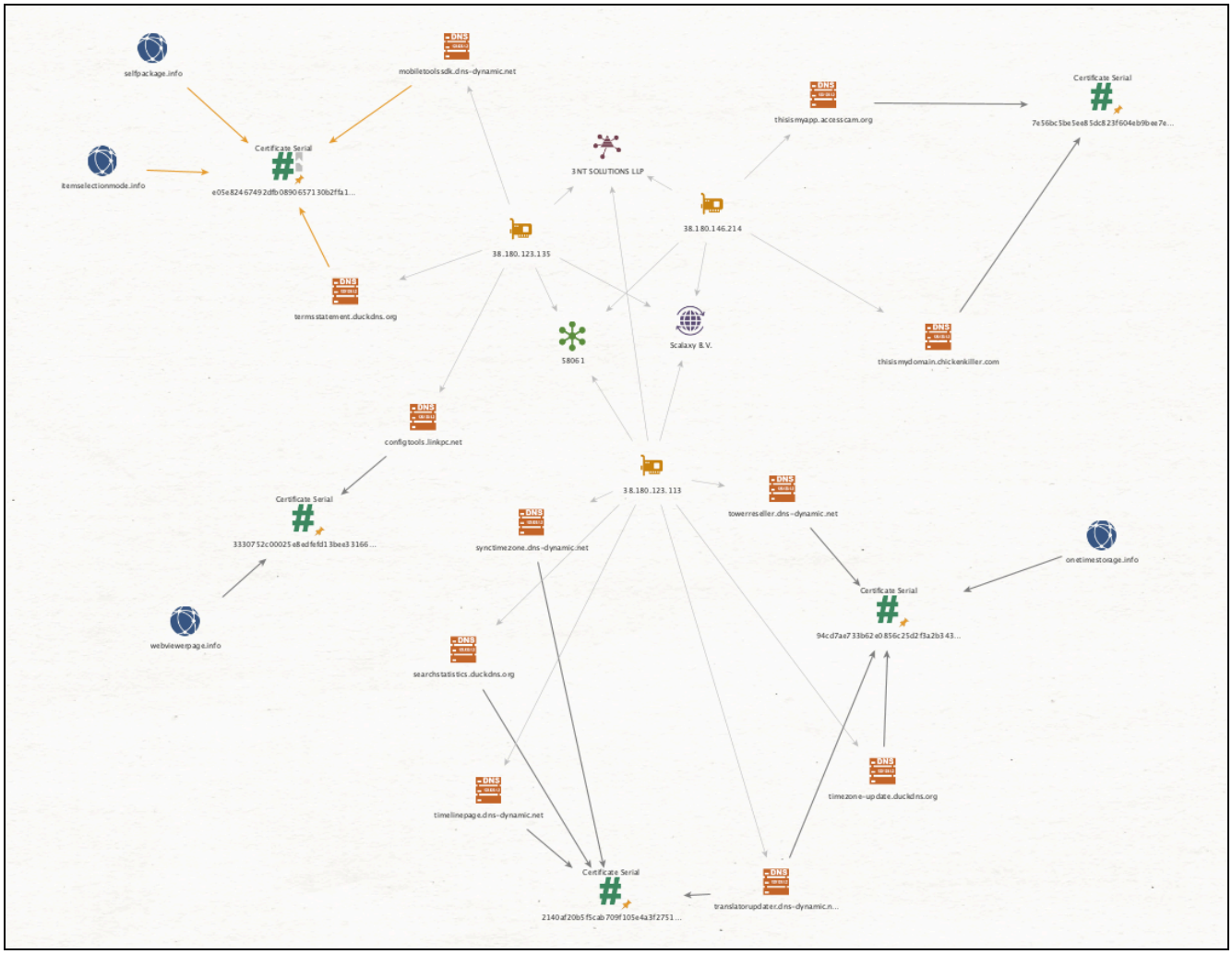

Figure 1: *Link analysis between DDNS domains revealed a direct relationship via TLS certificates and reliance on the same infrastructure provider (Source: Recorded Future)*

As depicted in **Figure 1**, many of the DDNS domains identified as part of the research also shared TLS certificates with other domains connected to the same cluster. As of this writing, the overwhelming majority were issued Let's Encrypt certificates throughout the June, July, and August 2024 research periods.

We observed that many of these domains shared the same HTML splash page of an unrelated food and beverage group (**Figure 2**), which is likely an indicator of domain parking prior to or after operationalization. We observed HTML splash pages in two other instances, including a Sudoku-themed page associated with one DDNS domain and two other domains hosted on *172.86.77[.]85* (**Figure 2**). The server configurations of the GreenCharlie infrastructure suggest that two other IPs — *38.180.146[.]219* and *45.137.213[.]145* — shared the same configurations. It is likely the two additional domains are also linked to the large cluster of GreenCharlie infrastructure.

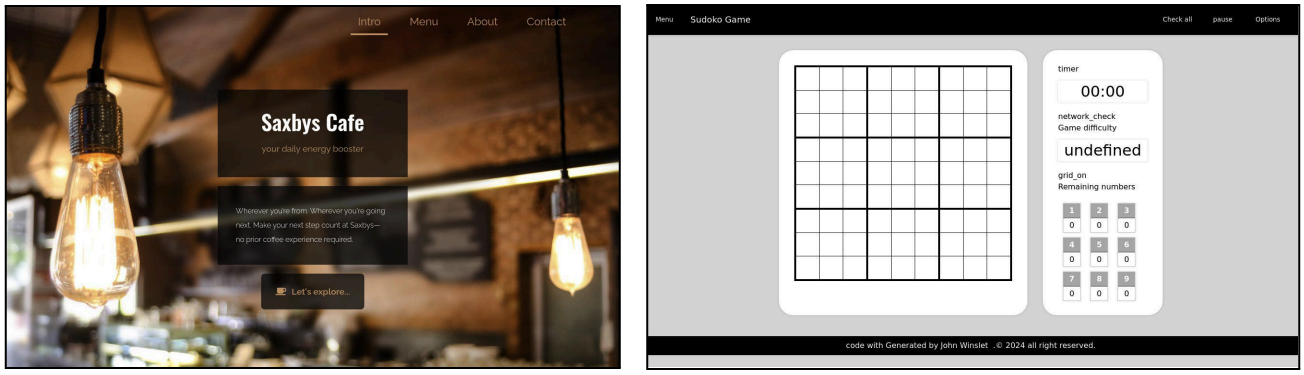

Figure 2: *GreenCharlie domains shared the same HTML splash page (Source: DomainTools, URLScan)*

Network Intelligence Observations

Suspected Tiered Structure

Analysis of Recorded Future Network Intelligence revealed a likely tiered communication structure between the IP addresses identified as part of this research. From July 25, 2024, until the time of this writing, we observed that specific IP addresses hosting GreenCharlie domains, including *38.180.123[.]113*, *38.180.123[.]135*, *38.180.146[.]194*, *38.180.146[.]174*, *172.86.77[.]85,* and *185.241.61[.]86*, communicated over ports such as 8624, 8647, 7564, and 1456 with various other IP addresses, some of which are suspected of being linked to the same infrastructure.

Communication with Iran-based IP Addresses

Throughout July and August 2024, Recorded Future Network Intelligence depicted Iran-based IP addresses communicating with GreenCharlie's infrastructure, such as the IP address *38.180.146[.]194* and *38.180.146[.]174* (**Figure 3**).

To verify the suspicious nature of the Iranian IP addresses we compared the network traffic patterns with that observed among GreenCharlie IP addresses. As noted above, from July 25, 2024, until the time of this writing, GreenCharlie infrastructure communicated extensively over specific ports such as 8624. Over the same time period, IP addresses hosting GreenCharlie domains also communicated with the following Iranian IP addresses over port 8624:

- *37.148.63[.]24*
- *93.119.48[.]60*
- *5.106.153[.]245*
- *5.106.169[.]235*
- *5.106.185[.]98*
- *5.106.202[.]101*
- *5.106.219[.]243*

We also observed Iran-based IP addresses communicating over ports 443 and 80 with GreenCharlie infrastructure. In some cases, the IP addresses included those from the same local network; for example, *185.166.104[.]3* and *185.166.104[.]4*. This could suggest threat actors operating from nearby workstations engaging with phishing infrastructure, or domestic navigation to the IP addresses, potentially as part of internal targeting activity. Both IP addresses are owned by the entity Avaye Hamrahe Houshmande Hezardastan (AS202319).

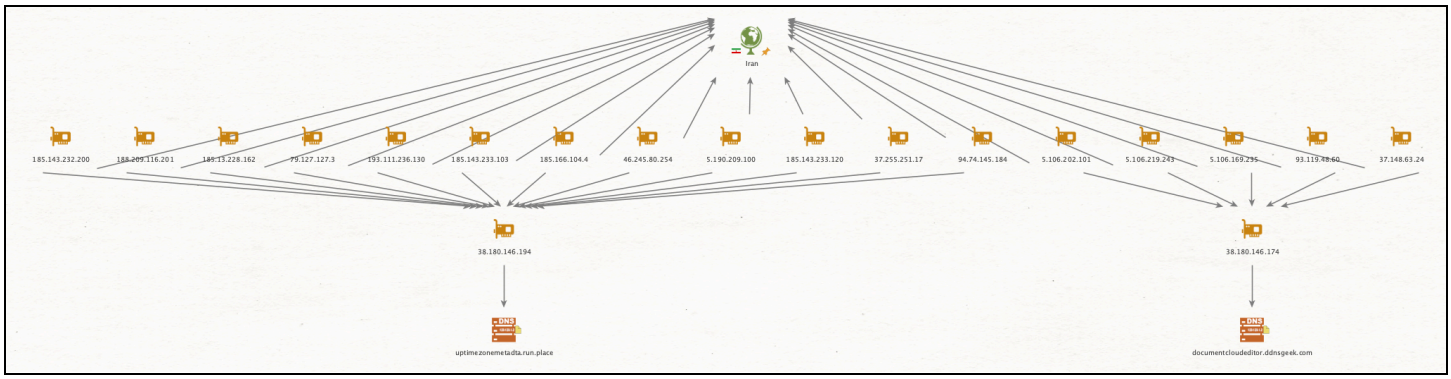

Figure 3: *From July 25, 2024, until the time of this writing, Iran-based IP addresses communicated with infrastructure likely associated with GreenCharlie (Source: Recorded Future)*

Phishing Link

From June 18, 2024, onward, we observed two domains resolving to *38.180.146[.]174* and *38.180.146[.]194*, *documentcloudeditor.ddnsgeek[.]com* and *uptimezonemetadta.run[.]place*, respectively. A submission to URLScan made on June 18, 2024, suggests a PhishTest portal was hosted on *38.180.146[.]174* (**Figure 4**). The domain was issued a Let's Encrypt certificate on the same day.

While we can't confirm that the phishing page was created or accessed by GreenCharlie threat actors, the domain does match GreenCharlie's known domain registration naming conventions. Furthermore, it is unclear whether PhishTest was used for attack operations, threat actor training, or Iran-based security awareness training. Recorded Future Network Intelligence was not used at the time of the URL submission to facilitate additional network intelligence research.

Regarding *uptimezonemetadta.run[.]place,* while we have not identified an "A" DNS record or TLS certificate associated with the domain, a submission to VirusTotal on July 29, 2024, suggests it pointed to *38.180.146[.]194*. Recorded Future Network Intelligence revealed that *38.180.146[.]194* communicated with other GreenCharlie infrastructure, including *38.180.123[.]113* and *172.86.77[.]85*, between July 28 and July 30, 2024. Based on these links we assess this was highly likely a phishing portal associated with the same threat activity.

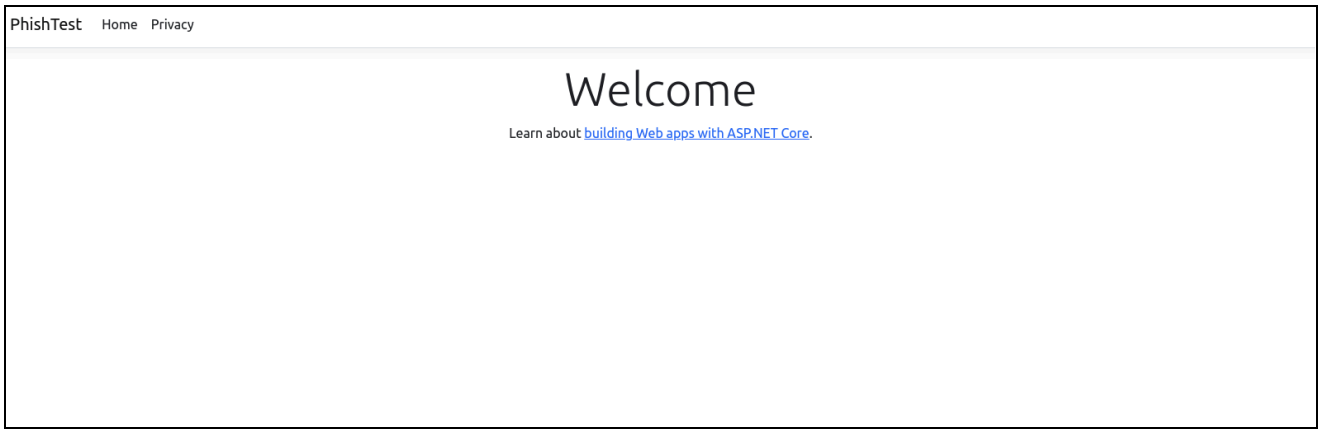

Figure 4: *Scanned domain documentcloudeditor.ddnsgeek[.]com resulted in the observed PhishTest portal (Source: URLScan)*

We also note that during the same timeframe, network traffic depicting full or half handshakes was observed over ports 445 and 443 with Iran-based IP addresses, which included *193.111.236[.]130*, *94.74.175[.]209*, *185.143.233[.]120*, *94.74.145[.]184*, and *37.255.251[.]17*. We note the possibility that some of the IP addresses associated with port 445 communications are unrelated to this research, and may be linked to scanning activity. However, based on the server configurations of *38.180.146[.]194* on July 29, 2024, port 445 was enabled by the administrator, and therefore this could be an indicator of a legitimate session.

Use of VPN Service

Recorded Future Network Intelligence also depicted consistent traffic between GreenCharlie infrastructure and IP addresses associated with the ProtonVPN and Proton mail service provider. These included the following IP addresses: *185.159.159[.]140*, *185.70.42[.]45*, *185.159.159[.]148*, *185.70.42[.]37*, *149.22.84[.]139*, *146.70.174[.]66*, *146.70.194[.]50*, and *169.150.226[.]161*. Queries (1, 2, 3, 4, 5, 6, 7, 8) of the IP addresses via the internet scanning service Shodan suggest the Proton servers are geolocated to Germany, the US, Israel, and France.

The use of VPN services to obfuscate their activity is common among different Iranian APTs. We have observed GreenCharlie use various other services in the past, such as ExpressVPN and PIA. However, on occasion these groups also experience operational security mishaps, which lead to cyber researchers more clearly detailing instances where Iranian IPs, almost certainly associated with an attacker's host, have been identified communicating with a victim network.

Malware Linked to GreenCharlie Infrastructure

Insikt Group identified significant code overlaps among the GORBLE, TAMECAT, and POWERSTAR (also known as CharmPower and GorjolEcho) malware families, strongly suggesting they are variants of the same family. **Figure 5** highlights these overlaps, particularly across the initial three stages of each

malware's infection chain. We note that Google-Mandiant has linked TAMECAT to threat activity associated with APT42. Insikt Group tracks infrastructure that overlaps with APT42 as GreenBravo.

In the first stage, all three families employ a similar function to decode a URL, which is used to fetch the next stage. Both GORBLE and TAMECAT hardcode a Mozilla user-agent header for the request, whereas POWERSTAR relies on the WebClient's default user agent. The response is Base64-decoded into a byte array, followed by a bitwise NOT operation on each byte to produce a PowerShell function (either `KeyMaster` or `Borjol`). This function is subsequently invoked within the script.

The second stage contains a single function that uses a hard-coded key and initialization vector (IV) to decrypt the payload from the first stage using AES encryption. Once decrypted, the payload is executed via the `Invoke-Expression` cmdlet. Additionally, this stage sets the C2 address and AES key used for C2 communications with the final payload. The stage two payloads of TAMECAT and POWERSTAR are nearly identical, differing only in hard-coded elements such as the C2 address, AES key, and IV used for C2 communication. GORBLE's version of stage two, however, replaces placeholder values in the decrypted payload with hard-coded values and executes it using `ScriptBlock.Create` instead of `Invoke-Expression`.

In the third stage, each malware family contacts the C2 server by sending a unique identifier hard-coded in the script, along with the victim's operating system and computer name. This information is formatted as JSON, encrypted, Base64 encoded, and transmitted via an HTTP POST request to the C2 server.

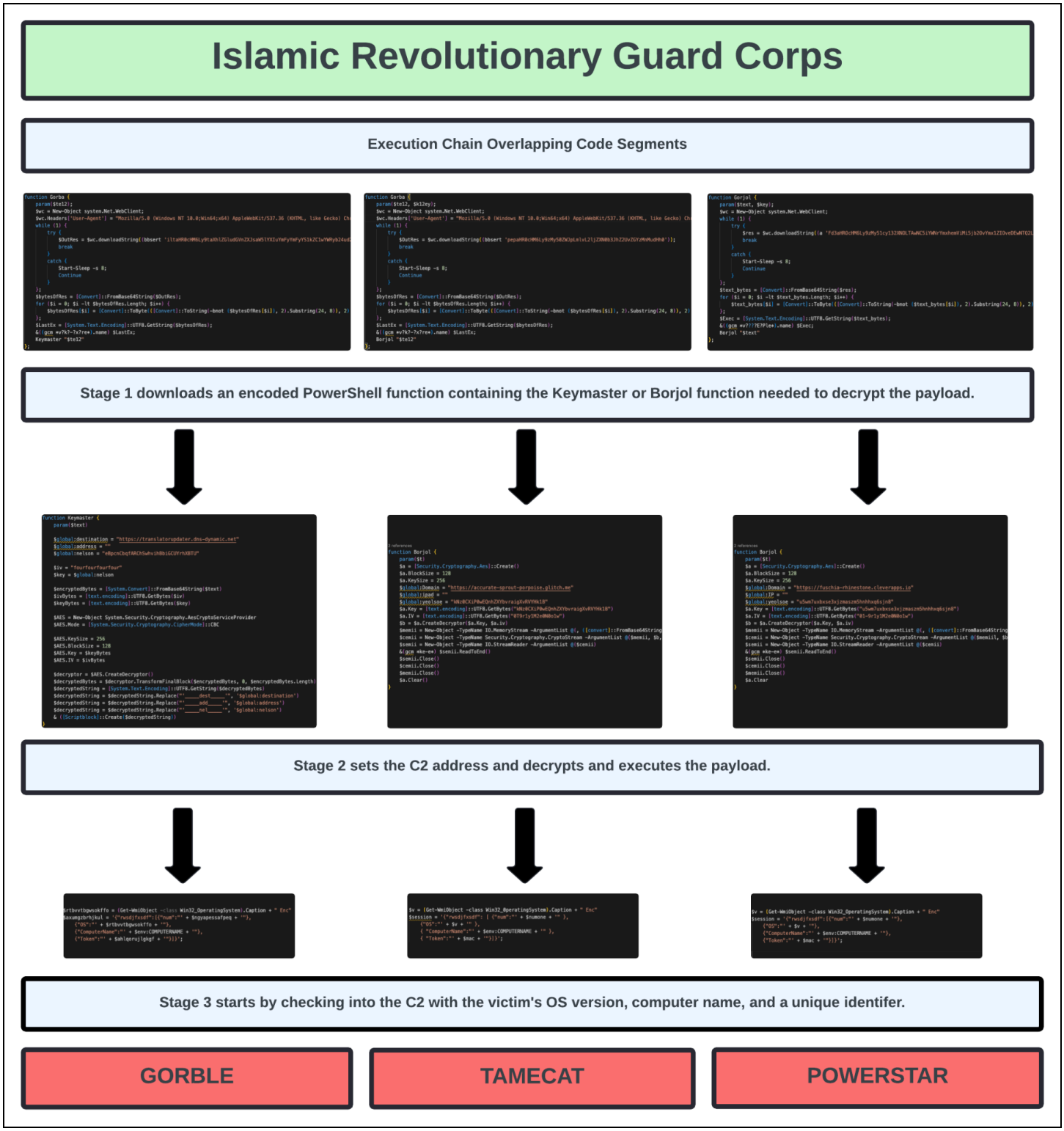

Figure 5: *Code overlaps between GORBLE, TAMECAT, and POWERSTAR malware (Source: Recorded Future)*

SHA256 Hash	C2 Domain	IP Address	First Seen
n/a	coldwarehexahash.dns-dynamic[.]net	38.180.123[.]231	2024-08-14
n/a	readquickarticle.dns-dynamic[.]net	38.180.123[.]231	2024-08-14
n/a	uptime-timezone.dns-dynamic[.]net	38.180.123[.]231	2024-07-20
c3486133783379e13ed37c45dc6645cbee4c1c6e62e7988722931eef99c8eaf3	translatorupdater.dns-dynamic[.]net	38.180.123[.]113	2024-06-16

Table 1: *A small sample of second-stage C2s identified by Insikt Group is part of the broader infrastructure cluster established by GreenCharlie (Source: Recorded Future)*

Attribution

Insikt Group tracks Iran-nexus threat activity clusters via specific infrastructure fingerprinting methodologies. Since we started tracking GreenCharlie, we have observed them linked to attack operations predominantly associated with strategic intelligence-gathering, as well as surveillance activity. Insikt Group tracks GreenCharlie in close proximity with threat activity tied to GreenBravo and GreenDelta (formerly TAG-56). We assess that all three groups share a strategic nexus to the Islamic Revolutionary Guard Corps (IRGC), in particular to that organization's intelligence wing (IRGC-IO).

Outlook

GreenCharlie remains highly active at the time of this writing, and while Insikt Group has not identified direct evidence of targeting against the US government or political parties, we assess that there is an elevated chance of attacks using the infrastructure listed in this report. On August 14, 2024, Google-Mandiant issued a report citing that it had identified and intercepted attempts to target individuals associated with US political campaigns. Based on the IoCs released by Google-Mandiant, we were able to identify a direct infrastructure correlation with our GreenCharlie research.

It is highly likely that the observations and subsequent analysis conducted via Recorded Future Network Intelligence point to Iranian threat actors engaging with the indicators listed in this report. While our research will continue to examine the domains, infrastructure, network intelligence, and malware, we recommend that interested parties pay increased attention to the traditional avenues Iranian APTs use to target their victims, which is predominantly via social engineering and spearphishing emails. Iranian APTs like to directly engage with targets via encrypted chats, SMS, and video calls to deliver malicious files. As of this writing, we have not identified evidence of vulnerability exploitation, even though historical cases indicate that elements associated with the IRGC's cyber wing have exploited vulnerabilities (Log4j, among others) to target systems.

Appendix A — Indicators of Compromise

Domains:

activeeditor[.]info
personalwebview[.]info
longlivefreedom.ddns[.]net
hugmefirstddd.ddns[.]net
icenotebook.ddns[.]net
softservicetel.ddns[.]net
configtools.linkpc[.]net
webviewerpage[.]info
www.selfpackage[.]info
selfpackage[.]info
itemselectionmode[.]info
termsstatement.duckdns[.]org
mobiletoolssdk.dns-dynamic[.]net
researchdocument[.]info
timelinepage.dns-dynamic[.]net
searchstatistics.duckdns[.]org
messagepending[.]info
www.chatsynctransfer[.]info
synctimezone.dns-dynamic[.]net
chatsynctransfer[.]info
timezone-update.duckdns[.]org
onetimestorage[.]info
towerreseller.dns-dynamic[.]net
translatorupdater.dns-dynamic[.]net
api.overall-continuing[.]site
backend.cheap-case[.]site
admin.cheap-case[.]site
demo.cheap-case[.]site
dev.cheap-case[.]site
app.cheap-case[.]site
api.cheap-case[.]site
editioncloudfiles.dns-dynamic[.]net
fileeditiontools.linkpc[.]net
entryconfirmation.duckdns[.]org
doceditor.duckdns[.]org
projectdrivevirtualcloud.co[.]uk
continueresource.forumz[.]info
destinationzone.duia[.]eu
onlinecloudzone[.]info
storageprovider.duia[.]eu
lineeditor.32-b[.]it
lineeditor.001www[.]com
lineeditor.mypi[.]co
dynamicrender.line[.]pm
nextcloudzone.dns-dynamic[.]net
realpage.redirectme[.]net
sharestoredocs.theworkpc[.]com
thisismyapp.accesscam[.]org

thisismydomain.chickenkiller[.]com
pagerendercloud.linkpc[.]net
splitviewer.linkpc[.]net
pageviewer.linkpc[.]net
preparingdestination.fixip[.]org
joincloud.mypi[.]co
joincloud.duckdns[.]org
realcloud[.]info
directfileinternal[.]info
sourceusedirection.mypi[.]co
viewdestination.vpndns[.]net
overflow.duia[.]eu
tracedestination.duia[.]eu
continue.duia[.]eu
linereview.duia[.]eu
highlightsreview.line.pm
nextcloud.duia[.]us
smartview.dns-dynamic.net
contentpreview.redirectme[.]net
finaledition.redirectme[.]net
dynamictranslator.ddnsgeek[.]com
personalstoragebox.linkpc[.]net
personalcloudparent[.]info
cloudarchive[.]info
cloudregionpages[.]info
streaml23.duia[.]eu
pkglessplans[.]xyz
worldstate.duia[.]us
callfeedback.duia[.]ro
reviewedition.duia[.]eu
filereader.dns-dynamic[.]net
vector.kozow[.]com
cloudtools.duia[.]eu
uptimezonemetadta.run[.]place
documentcloudeditor.ddnsgeek[.]com
coldwarehexahash.dns-dynamic[.]net
readquickarticle.dns-dynamic[.]net
uptime-timezone.dns-dynamic[.]net

IP Addresses:
185.241.61[.]86
172.86.77[.]85
146.70.95[.]251
91.232.105[.]185
54.39.143[.]112
38.180.91[.]213
38.180.123[.]135
38.180.123[.]113
38.180.123[.]187
38.180.146[.]214
38.180.146[.]212
38.180.146[.]194

38.180.146[.]174
38.180.123[.]231
38.180.123[.]234
38.180.146[.]252
37.1.194[.]250

Iran-based IP Addresses:
193.111.236[.]130
185.143.233[.]120
94.74.175[.]209
94.74.145[.]184
93.119.48[.]60
37.148.63[.]24
37.255.251[.]17
5.106.153[.]245
5.106.169[.]235
5.106.185[.]98
5.106.202[.]101
5.106.219[.]243

Malware Hash:
C3486133783379e13ed37c45dc6645cbee4c1c6e62e7988722931eef99c8eaf3
33a61ff123713da26f45b399a9828e29ad25fbda7e8994c954d714375ef92156
4ac088bf25d153ec2b9402377695b15a28019dc8087d98bd34e10fed3424125f

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Establish Accounts: Email Accounts	T1585.002
Initial Access: Spearphishing Attachment	T1566.001
Initial Access: Spearphishing Link	T1566.002
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Command and Scripting Interpreter: Unix Shell	T1059.004
Persistence: Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder	T1547.001
Persistence: Scheduled Task/Job: Scheduled Task	T1053.005
Discovery: System Information Discovery	T1082
Discovery: Process Discovery	T1057
Command and Control: Application Layer Protocol: Web Protocols	T1071.001

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com