

Bomgar : Prise de contrôle contrôlée

Fabrice Prigent

Université Toulouse 1 Capitole

Jeudi 27 février 2014

Université en sciences sociales

- 20000 inscriptions
- 1100 personnels (permanents ou contractuels "présents")
- 3 sites sur 1 km de distance
 - L'Arsenal
 - Les anciennes facultés.
 - La Manufacture des tabacs
- Des délocalisations étrangères
 - Maroc
 - Vietnam
 - Vanuatu
 - etc.
- Des VIPs en déplacement permanent

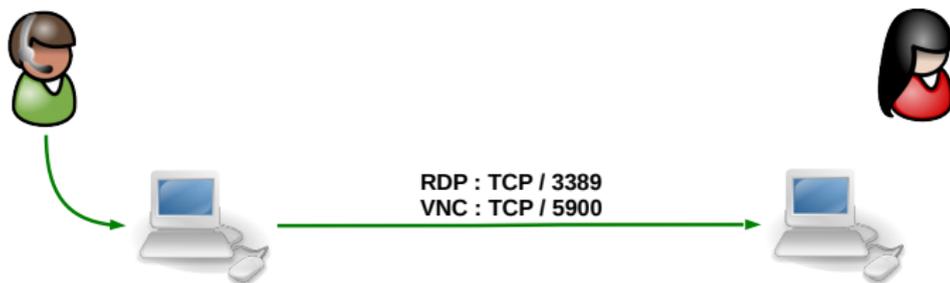
Le parc

- 1400 ordinateurs fixes
 - majoritairement pour les personnels et les étudiants
- 300 ordinateurs portables
 - majoritairement pour les responsables et les enseignants-chercheurs.
- Des postes "inventoriés non gérés" en progression
 - des Windows (version officielle +1, +2),
 - des Macs,
 - des Linux,
 - des smart/i/samsung/nimportenawak "phones" ou "tab".

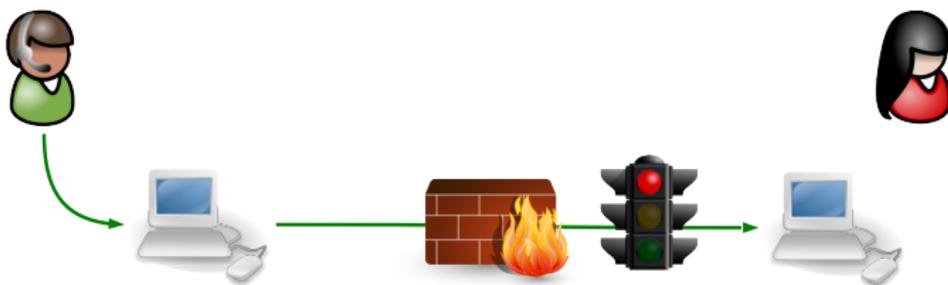
Les interventions

- Une structure centralisée (le 3636)
- 10 personnes pour le support
 - 2 personnes dédiées à l'accueil (niveau 0,1 ITIL)
 - 3 dédiées aux interventions (niveau 2 ITIL)
 - Déplacement sur place
 - Utilisation de VNC (UltraVNC)
 - 7000 interventions par an.

La prise de contrôle classique



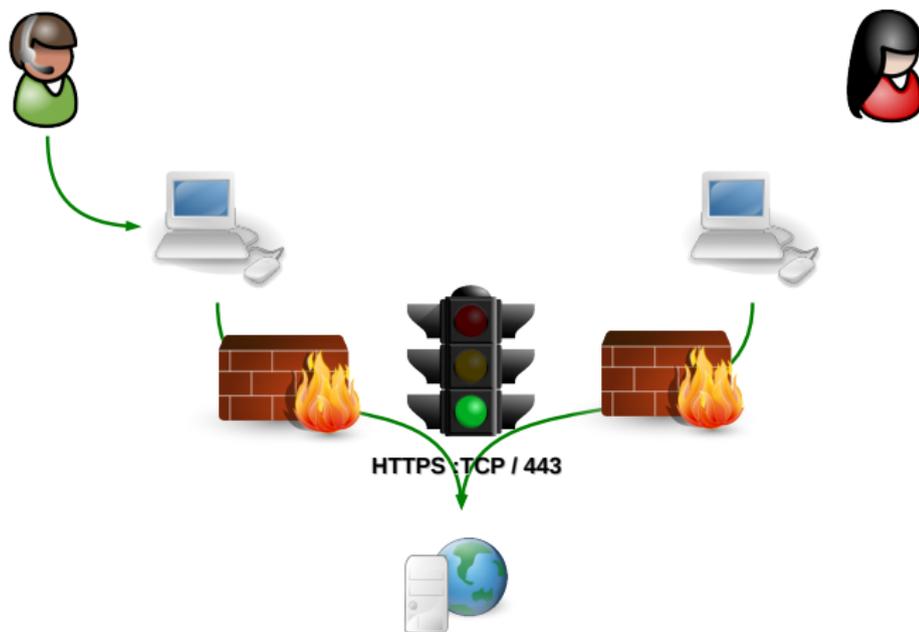
La prise de contrôle classique : avec firewall



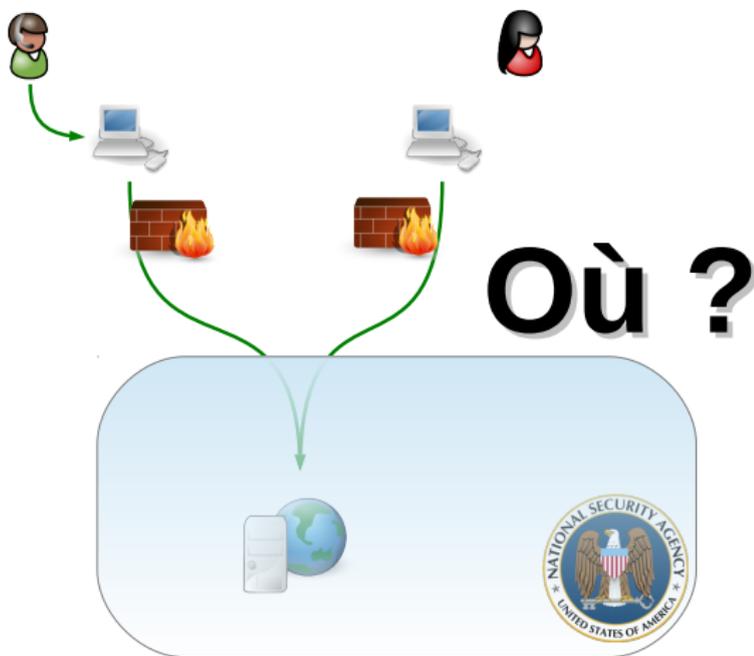
La prise de contrôle sans firewall

DNS	IP	Attaque	Nb
xxxxx.powerhost.ro	93.114.46.160	Scan de port rdesktop	24492
adsl-98-71-245-112.jax.bellsouth.net	98.71.245.112	scan POP3	2998
richard.tcn.net	199.166.4.8	scan POP3	2604
41334f34.cst.lightpath.net	65.51.79.52	Scan de port rdesktop	2120
59.67.71.233	59.67.71.233	Scan de port rdesktop	1718
208.151.198.203.static.netvigator.com	203.198.151.208	scan POP3	1351
whitney.portmorgan.com	208.92.64.5	Scan de port rdesktop	1154
75-146-0-66-delmarva.hfc.comcastbusiness.net	75.146.0.66	Scan de port rdesktop	883
dsl-200-67-153-188-sta.prod-empresarial.com.mx	200.67.153.188	Scan de port rdesktop	565
188.212.152.4	188.212.152.4	Scan de port rdesktop	292
116.32.124.158	116.32.124.158	scan POP3	275
95-143-134-116.client.tltnet.cz	95.143.134.116	Scan de port actif telnet	136
ns1.mcsi.ro	80.96.196.3	Scan de port rdesktop	131
122-117-227-190.hinet-ip.hinet.net	122.117.227.190	Scan de port actif telnet	129
mom77-1-88-179-134-18.fbx.proxad.net	88.179.134.18	Scan de port actif telnet	115
acgr158.neoplus.adsl.tpnet.pl	83.9.245.158	Scan de port actif telnet	112
220-135-67-78.hinet-ip.hinet.net	220.135.67.78	Scan de port actif telnet	112
202-18-137-186.fibertel.com.ar	186.137.18.202	Scan de port actif telnet	111
server109-228-24-147.live-servers.net	109.228.24.147	Scan de port rdesktop	100
122.199.99.232	122.199.99.232	Scan de port actif telnet	99
sab57-4-88-164-211-233.fbx.proxad.net	88.164.211.233	scan POP3	94
220-134-182-16.hinet-ip.hinet.net	220.134.182.16	Scan de port actif telnet	78
host-92-26-192-174.as13285.net	92.26.192.174	Scan de port actif telnet	77
122-117-29-122.hinet-ip.hinet.net	122.117.29.122	Scan de port actif telnet	71
68-188-15-166.static.stls.mo.charter.com	68.188.15.166	Scan de port rdesktop	70
host68-171-149-62.serverdedicati.aruba.it	62.149.171.68	Scan de port rdesktop	60
fax.harboraccess.com	69.57.56.26	Scan de port rdesktop	55
pa42-241-22-24.pa.nsw.optusnet.com.au	42.241.22.24	scan POP3	51

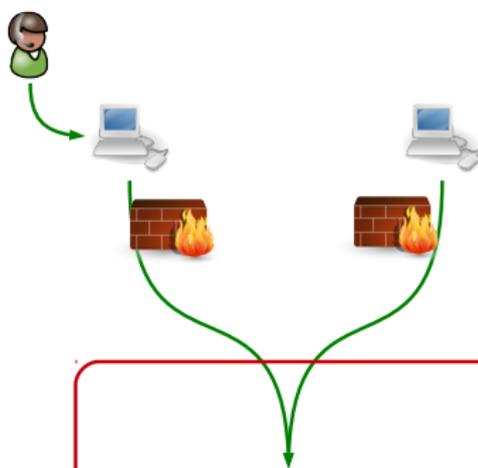
La prise de contrôle déportée



La prise de contrôle déportée : où ?



La prise de contrôle déportée : où ?



Chez Nous !



Des usages qui évoluent

- De plus en plus de portables
 - avec station d'accueil et écran de grand dimension (double écran)
 - avec une utilisation à la maison (par des lignes ADSL plus ou moins rapides)
- Généralisation des postes "non administrateurs"
 - installation de logiciels par la DSI
 - installation de composants par la DSI.

Des contraintes plus fortes

- Webification des applications
 - VNC gère très mal les navigateurs.
- Effet "PRISM"
 - Problématique de la prise de contrôle en passant par des serveurs étrangers.

Des constantes

- Plus la technologie avance, et moins les utilisateurs comprennent
- Plus la technologie avance, et plus la simplification donne l'impression aux utilisateurs qu'ils comprennent.
 - donc, ils veulent faire plus de choses
 - donc, ils font plus de ... manipulations inappropriées.

Nos demandes

- Passer les firewalls "simplement" (HTTP/HTTPS),
- Etre en mesure de gérer des postes à distance sur des lignes bas débit,
- Simplicité de déploiement (pour les utilisateurs, y compris Tata Jostette),
- Contrôler la chaîne de prise de contrôle,
- Passage en mode administrateur,
- Gestion du double écran.

Tests

Nous avons testé longuement chacun des concurrents potentiels.

- Dans les conditions d'utilisation demandées (ADSL)
- Avec les produits définitifs (logiciels ou matériels)

And the Winner is



- Parce qu'il est au même niveau que les leaders (logiciels) du marché sur les fonctionnalités.
 - Logmeln
 - TeamViewer
- Mais qu'il est le seul, distribué en europe, à le faire sous notre contrôle. Un autre logiciel (streamconnect), sur le marché américain semble être en mesure de le faire.
- Parce que les versions du client sont toujours adaptées à la version du matériel.

Principes de fonctionnement

- Principe d'appliance (possibilité de SaaS, et de VM)
- Connexions sortantes en HTTPS (compatibilité maximale avec les Pare-feu)
 - pour l'informaticien
 - pour l'utilisateur
- En "one-shot" non préparé
 - l'informaticien génère un code sur la plateforme
 - l'utilisateur va sur l'url `http://sos.ut-capitole.fr/`
 - il entre le code
 - il télécharge le client
- Si le poste est préparé
 - Installation d'un bouton d'appel
 - Installation transparente d'un lancement de client (notion de jump client).

Des clients

- Distribution des logiciels de prise en main
 - par HTTPS
 - depuis le boitier
 - pour l'informaticien et l'utilisateur
- Pour tous les OS (pour informaticien et utilisateur)
 - Windows
 - Mac/OS
 - Linux
 - Android (en lecture seule pour le client)
 - IOS (avec restrictions malgré tout)

Les fonctions

- Prise de contrôle
- Transfert de fichiers
- Informations système
- Chat
- Lancement de commandes en mode administrateur

La gestion des licences

- Achat d'un boîtier (B200 pour nous), moins de 2000 €.
- Achat de licences simultanées d'utilisation
 - suivant le mode (entreprise ou standard)
 - en gros le prix du boîtier
- Maintenance
 - 15% par an
 - Elle n'est pas obligatoire (le client n'a pas d'upgrade forcé)
- En cours de validation par le "Groupe Logiciel" du MESR.

Support : Portail

The screenshot shows a Mozilla Firefox browser window with the title "CONNEXION | Bomgar - Mozilla Firefox". The address bar displays the URL "https://sos.ut-capitole.fr/login/login.ns?redirect=%2Flogin%". The page content includes the "BOMGAR™" logo in orange and the "CONNEXION" logo with a globe icon and a language dropdown menu set to "Français". Below the logos is a dark grey header with the word "Connexion" in white. The main form area contains two input fields: "Nom d'utilisateur" and "Mot de passe", both with light blue borders. Below these fields is an orange button labeled "Connexion". At the bottom of the form area, a horizontal line is followed by the text "Les cookies doivent être activés pour se connecter". A footer bar at the bottom of the page contains the text "Copyright © 2002-2012 Bomgar Corporation. Redistribution interdite. Tous droits réservés."

Le contexte
Les interventions
La prise de contrôle pour les tout petits
Un contexte qui change
Bomgar
Conclusion

Exemple d'une session "One-Shot"
Les modes de connexions
Les autorisations
Des précautions

Support : Portail

The screenshot shows the Bomgar user portal interface. At the top, there is a navigation bar with the Bomgar logo on the left and the text "CONNEXION UTILISATEUR" on the right. Below the navigation bar, there is a menu with various options: ÉTAT, MON COMPTE, CONFIGURATION, UTILISATEURS & SÉCURITÉ, RAPPORTS, PUBLICPORTAL, LOCALISATION, GESTION, INFORMATIONS, TECHNICIENS D'ASSISTANCE, and NOUVEAUTÉS. The main content area is titled "État du site" and displays various system status information:

- Nom d'hôte principal: sos.ut-capitole.fr
- Société/nom de division: Université de Toulouse
- Nom de produit: Bomgar
- Version du produit: 12.3.5
- Build du produit: 43325
- Version de l'API: 1.0.0
- GUID du serveur Bomgar: 9e759bbbf094d1c964c77b670f6e036
- Temps de fonctionnement du système: 213 jour(s), 7 heure(s) et 19 minute(s)
- Processus: 0.00, 0.00, 0.00 (0)
- État du diagnostic: 0
- Heure du système: sam 22 fév 2014 18:20:19 CET
- Fuseau horaire: Europe/Paris
- Nombre total de Jump Clients actifs autorisés: 1000
- Nombre total de Jump Clients passifs autorisés: 1000
- Licences d'assistance technique complètes: 6 Standard
- Acheter des licences supplémentaires: [Acheter](#)
- Redémarrer le logiciel Bomgar: [Redémarrer](#)
- Ce logiciel client est paramétré pour se connecter à: sos.ut-capitole.fr:443
- Clients connectés:

Nom du client	Compte
Console du technicien d'assistance Bomgar	1
Total :	1

Support : Téléchargement

BOMGAR™ CONNECTION UTILISATEUR

Français | Interface d'administration | PRIGENT FABRICE | DÉCONNEXION

ÉTAT | MON COMPTE | CONFIGURATION | UTILISATEURS & SÉCURITÉ | RAPPORTS | PUBLICPORTAL | LOCALISATION | GESTION

Console du technicien d'assistance Bomgar

Choisir une plate-forme :

Télécharger Console du technicien d'assistance Bomgar

Suivez cette procédure pour la connexion initiale à la Console du technicien d'assistance Bomgar :

1. Téléchargez et « Ouvrez » le logiciel de la console.
2. Installez le logiciel grâce à l'assistant d'installation.
3. Une fois l'installation terminée, une icône apparaîtra dans votre barre système et une invite de connexion apparaîtra sur votre écran. Si cette dernière n'apparaît pas, cliquez avec le bouton droit sur l'icône dans la barre système et sélectionnez « Ouvrir une session ».
4. Indiquez votre nom et votre mot de passe pour vous connecter.

Console du technicien d'assistance Bomgar Installeur de déploiement en masse

Choisir une architecture Windows® :

Télécharger la Console du technicien d'assistance Bomgar MSI

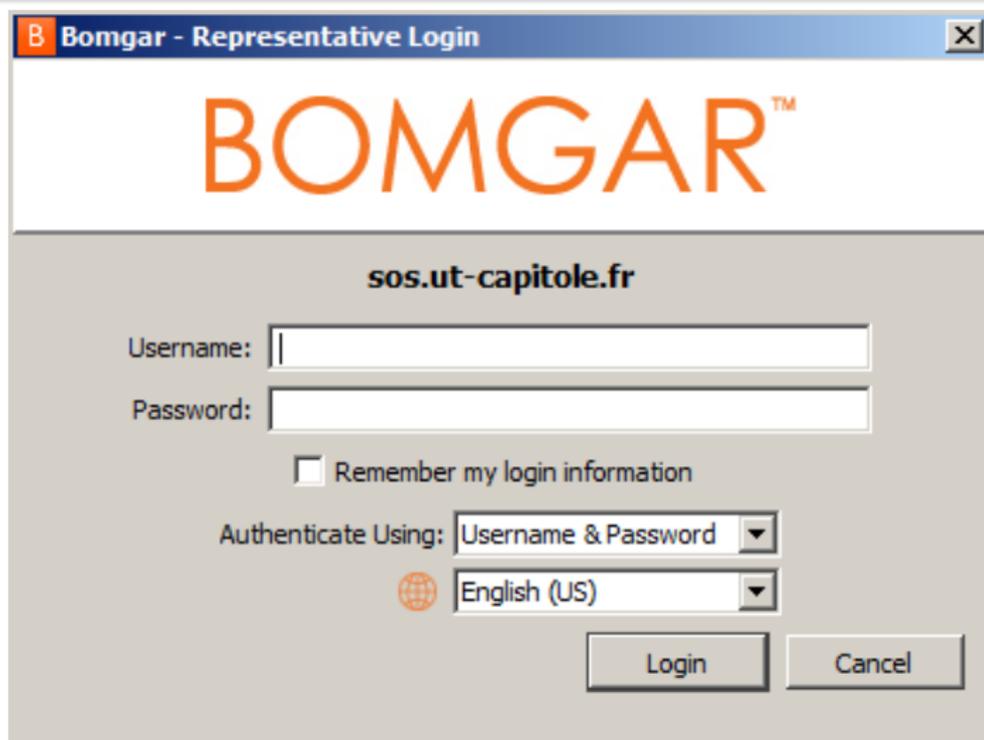
Suivez cette procédure pour déployer la Console du technicien d'assistance Bomgar :

1. Téléchargez le MSI.
2. À votre invite de commande, utilisez la commande suivante pour l'installer :

```
msiexec /i [nom du fichier].msi
```

Reportez-vous à votre documentation pour obtenir des arguments supplémentaires permettant de contrôler l'installation de la Console du technicien d'assistance Bomgar.

Support : Lancement du logiciel



The image shows a screenshot of a web browser window titled "Bomgar - Representative Login". The window displays the Bomgar logo in large orange letters. Below the logo, the URL "sos.ut-capitole.fr" is shown. There are two input fields: "Username:" and "Password:". Below these fields is a checkbox labeled "Remember my login information". Underneath is a dropdown menu labeled "Authenticate Using:" with "Username & Password" selected. Below that is another dropdown menu with a globe icon and "English (US)" selected. At the bottom right, there are two buttons: "Login" and "Cancel".

Support : Lancement du logiciel

The screenshot shows the Bomgar technician console interface. The title bar reads "Console du technicien d'assistance Bomgar - sos.ut-capitole.fr - PRIGENT FABRICE". The menu bar includes "Fichier", "Assistance technique", "Présentation", and "Aide".

At the top, there are buttons for "Démarrage...", "Shell Jump...", "Jump...", "Accepter", and "Transférer". Below these are tabs for "Personnelle (0)" and "Générale (0)".

The main area contains a table with the following columns: "Temps dans la file d'attente", "Nom", "Ordinateur", "Plate-forme", and "Problème". The table is currently empty.

Below the table are buttons for "Jump", "Supprimer", "Réfinir un groupe", "Exporter...", "Actualiser", and "Recherche...".

On the right side, there is a panel titled "Tous les techniciens d'assistance" which is currently empty. Below it, a list shows "Tous les techniciens d'assistance" and "LAUBERNY JEROME" with a button "Envoyer le fichier".

At the bottom left, there is a tree view showing "Tous les Jump Clients" with sub-items: "Personnelle", "Général", "Tier 1", and "Tier 2".

At the bottom right, there is a table with columns "Nom", "Commentaires", and "File".

Support : Choix d'une prise de contrôle

B Bomgar - Démarrer une session d'assistance technique

Choisissez l'une des options ci-dessous pour démarrer une session d'assistance technique :

Partager une clé de session

Demandez à un utilisateur distant de se rendre sur `sos.ut-capitole.fr` et de fournir cette **Clé de session générée** pour se connecter à

Envoyer un lien à un utilisateur par email

Demandez à un utilisateur distant de cliquer sur le lien figurant dans cet **E-mail** pour démarrer une session d'assistance technique.

Jump

Vous permet d'effectuer un Jump vers un système distant dépourvu d'opérateur.

Ceci va dédencher une tentative de Jump vers l'ordinateur distant que vous avez spécifié ici.

Pour y parvenir, vous devez disposer des droits d'administrateur sur la machine distante.

Jumpoint™ : Réseau local

Retenir Jumpoint™

Nom d'hôte / IP :

Jump

Support : Création d'un numéro de session

B Bomgar - Démarrer une session d'assistance technique

Choisissez l'une des options ci-dessous pour démarrer une session d'assistance technique :

Partager une clé de session

Demandez à un utilisateur distant de se rendre sur sos.ut-capitole.fr et de fournir cette **Clé de session générée** pour se connecter à v

Envoyer un lien à un utilisateur par email

Demandez à un utilisateur distant de cliquer sur le lien figurant dans cet **E-mail** pour démarrer une session d'assistance technique.

Jump

Vous permet d'effectuer un Jump vers u

Ceci va déclencher une tentativ
Pour y parvenir, vous devez disp

Jumpoint™ : Réseau local

Retenir Jumpoint™

Nom d'hôte / IP :

B Bomgar - Clé de session d'assistance technique [X]

 Clé de session : **5172486**

Expire le : 22 février 2014 18:44:17

OK

Jump

Utilisateur : Portail

The screenshot shows a web browser window titled "Portail d'assistance technique - Mozilla Firefox". The address bar contains "sos.ut-capitole.fr". The page header features the logo of "UNIVERSITÉ TOULOUSE 1 CAPITOLE" on the left and the text "PORTAIL D'ASSISTANCE TECHNIQUE" on the right, with a language dropdown menu set to "Français". Below the header is a dark grey bar labeled "Clé de session" with a question mark icon. Underneath is a text input field and an orange "Soumettre" button. At the bottom, it says "Powered By BOMGAR™" and "Logiciel d'accès à distance multiplateforme pour les services d'assistance technique".

Utilisateur : Rapatriement du client spécifique

Portail d'assistance technique - Firefox Fenêtre

Ma page personnelle | Portail d'assistance technique

UNIVERSITÉ TOULOUSE 1 CAPITOLE

PORTAL D'ASSISTANCE TECHNIQUE

Français

Vous êtes sur le point de commencer une session d'assistance technique avec PRIGENT FABRICE.

1. Exécutez le fichier que vous venez de télécharger. Si vous ne voyez pas le fichier, cliquez ici
2. Cliquez sur Exécuter si vous y êtes invité(e) pour exécuter ce logiciel.

Vous pouvez fermer cette fenêtre à tout moment après le démarrage de votre session.

Powered By
BOMGAR
Logiciel d'accès PC à distance pour les services d'assistance technique

Ouverture de bomgar-sec-0dc30d58bf77edhdjyfc716c40j90.exe

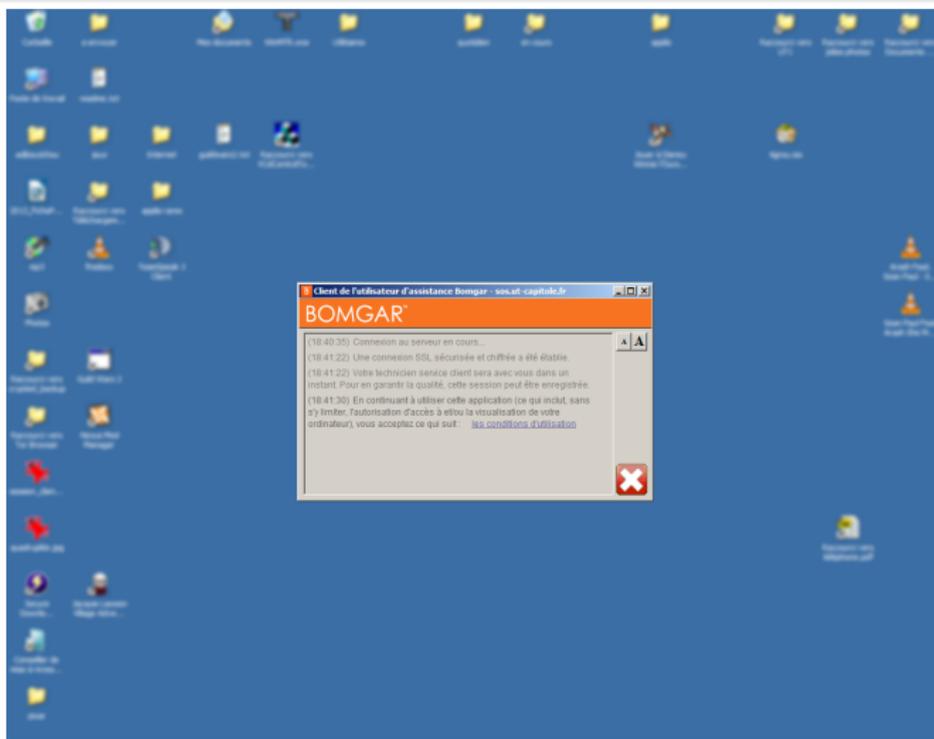
Vous avez choisi d'ouvrir :

- ...0dc30d58bf77edhdjyfc716c40j90.exe
qui est un fichier de type : Binary File (1,3 Mo)
à partir de : http://www.univ-toulouse.fr

Vouslez-vous enregistrer ce fichier ?

Enregistrer le fichier | Annuler

Utilisateur : Lancement du client

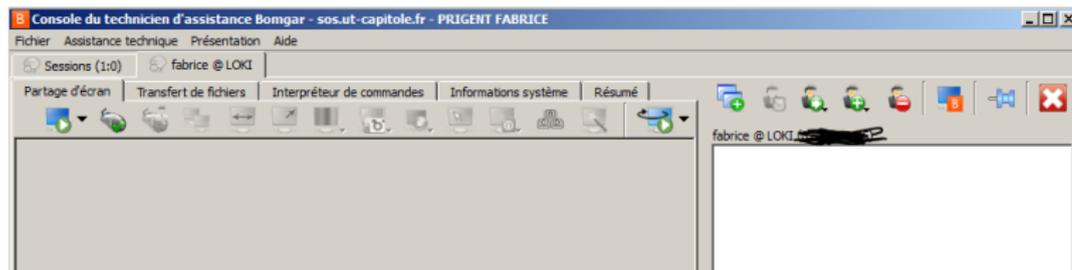


Support : visualisation de la session

The screenshot shows the Bomgar technician console interface. At the top, the title bar reads "Console du technicien d'assistance Bomgar - sos.ut-capitole.fr - PRIGENT FABRICE". Below the title bar, there are menu items: "Fichier", "Assistance technique", "Présentation", and "Aide". The main area is divided into sections. On the left, there are tabs for "Sessions (1:0)", "Personnelle (1)", and "Générale (0)". The "Sessions (1:0)" tab is active. In the center, there are several buttons: "Démarrage...", "Shell Jump...", "Jump...", "Accepter", and "Transférer". Below these buttons, there is a table with the following columns: "Temps dans la file d'attente", "Nom", "Ordinateur", "Plate-forme", and "Problème". The table contains one row of data:

Temps dans la file d'attente	Nom	Ordinateur	Plate-forme	Problème
0:01:50	fabrice	LOKI	Windows XP Hom...	

Session utilisateur



Session utilisateur

The screenshot shows a remote control session interface. The main window is titled "Console du technicien d'assistance Bomgar - sos.ut-capitole.fr - PRIGENT FABRICE". It features a menu bar (Fichier, Assistance technique, Présentation, Aide) and a toolbar with icons for various functions like "Partage d'écran", "Transfert de fichiers", "Interpréteur de commandes", "Informations système", and "Résumé". The central area displays a Windows desktop with various icons and a taskbar. A small window titled "Client de l'assistant de résolution Bomgar" is open, showing a log of events. On the right side, there is a chat window with the text: "fabrice @ LOKI (18:45:05) PRIGENT FABRICE peut maintenant voir et contrôler l'écran de l'utilisateur." Below the chat window are buttons for "Envoyer le fichier", "Envoyer un wizz", and "Charger l'URL". At the bottom right, there is a section for "Informations de session" containing a table of session data.

Données de session	
Temps passé dans cette file d'attente :	0:04:03
Temps passé dans le système :	0:04:36
Adresse IP :	[REDACTED]
Nom d'utilisateur :	fabrice
Nom de l'ordinateur :	LOKI
Plate-forme :	Windows XP Home...
Nom de la société :	
Langue :	Français
Détails :	

Session utilisateur

B Enquête de satisfaction du technicien d'assistance

Veillez remplir l'enquête de satisfaction suivante.

1. Was the Customer's issue resolved?
 Yes
 No
2. How effective was this session in satisfying the customer?
 Very Effective
 Somewhat Effective
 Somewhat Ineffective
 Very Ineffective
3. How effective was this session in decreasing your call duration?
 Very Effective
 Somewhat Effective
 Somewhat Ineffective
 Very Ineffective
4. Was using Bomgar better than the previous support method?

OK Annuler

Les modes de connexions

5 modes principaux :

- One-shot
- Bomgar Button
- Jump client passif
- Jump client actif
- JumpPoint

One-Shot

Présenté ci-dessus, en général pour un poste inconnu ou jamais traité

Bomgar Button

- C'est une "icone" placée soit par déploiement, soit "épinglée" lors d'un "one-shot"
- Quand on clique, il met dans la file d'attente d'un informaticien ou d'un groupe d'informaticiens, la demande d'intervention.
- Le bouton peut-être personnalisé par les administrateurs bomgar
 - pour un informaticien particulier
 - avec une icone particulière
 - pour une durée particulière
 - une heure
 - une semaine
 - ...
 - 5 ans

JumpClient

- C'est un "service" qui est déployé et lancé automatiquement
- L'informaticien prend directement la main sur le poste de l'utilisateur sans intervention de celui-ci
- Le jumpclient peut-être personnalisé par les administrateurs bomgar
 - pour un informaticien particulier (ou un groupe)
 - pour une personne particulière ou pour tous les utilisateurs
- Il existe en 2 modes
 - le mode actif
 - le mode passif

JumpClient Actif

- Le client se connecte automatiquement au serveur Bomgar
- Le nombre de sessions simultanées est limité par le serveur
 - 1.000 pour un B200
 - 5.000 pour un B300
 - 10.000 pour un B400
- Les sessions consomment de la CPU
- Le client peut-être n'importe où dans le monde
- Utile pour les informaticiens qui veulent, de chez eux, prendre le contrôle de leur PC de bureau (ne contourne pas les screensavers, mais attention à l'ouverture de l'accès!!)

JumpClient Passif

- Le client se signale automatiquement 1 fois par jour au serveur Bomgar
- Il faut contacter le client sur un port particulier pour déclencher la prise de contrôle
- Le nombre de sessions simultanées est limité par le serveur
 - 1.000 pour un B200
 - 5.000 pour un B300
 - 10.000 pour un B400
- Les sessions ne consomment quasiment pas de CPU

JumpPoint

- Nécessite des licences "entreprises".
- C'est un proxy, qui doit être installé sur une machine dédiée.
- Le jumpoint permet de prendre le contrôle des postes sur le broadcast.

Des précautions

Le logiciel est particulièrement paramétrable, surtout en terme de permissions. Les rôles sont les suivants :

- L'administrateur Bomgar : il peut tout et voit tout
- L'informaticien : un compte lui est associé et peut éventuellement
 - consulter,
 - manipuler,
 - déployer.
- La granularité
 - la totalité,
 - le groupe,
 - l'informaticien.

Des précautions

- Gérer des postes au Vanuatu avec 12 heures de décalage horaire ne signifie pas 24/24H !
- Bien choisir son mode d'intervention.
- Il peut faire beaucoup de choses, mais il faut choisir un périmètre :
 - SCCM permet la prise de contrôle de postes fixes locaux.
 - Bomgar peut faire du lancement automatique de scripts.
 - Bomgar fait de l'enquête de satisfaction.

Des avantages périphériques

- L'utilisateur sait QUI se connecte.
- Prise de contrôle par des sociétés extérieures avec enregistrement des sessions.
- Possibilité de "pousser" des prises de contrôle vers un "expert".
- Liaison avec le LDAP, un AD, mais aussi une base locale.
- Les clients sont disponibles sur le serveur.
- On peut faire des présentations 1 vers n (50) facilement.
- On peut "retourner" la session (le client voit l'écran de l'informaticien).
- Quasiment tout est paramétrable.
- Des API sont disponibles.

Conclusion

Bomgar

- est un des (rares) projets qui s'est déroulé sans difficulté,
- fait exactement ce qu'on lui demande,
- fait facilement ce qu'on lui demande,
- fait tellement de choses, que l'on ne peut tout mettre en place,
- permet de bloquer par filtrage url les autres services de prise de contrôle,
- a un bon ROI (estimation : 2 ans à condition que votre direction connaisse la notion de coût complet).

Mais

- il nécessite de bien réfléchir aux périmètres des divers outils de gestion de parc,
- il faut choisir correctement les modes de déploiement,
- la gestion des smartphones est perfectible,

Merci de votre attention

Des questions ?